An Engineering Study of Onboard Checkout Techniques

CR 115260

A GUIDE TO ONBOARD CHECKOUT
VOLUME II: ENVIRONMENTAL CONTROL AND LIFE SUPPORT

Huntsville

IBM

An Engineering Study of Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME II: ENVIRONMENTAL CONTROL AND LIFE SUPPORT

IBM NUMBER: 71W-00309

SEPTEMBER 1971

Prepared for the
National Aeronautics and Space Administration
Manned Spacecraft Center
Houston, Texas 77058

CONTRACT NUMBER NAS9-11189

IBM Federal Systems Division, Electronics Systems Center/Huntsville, Alabama

Table of Contents

Table of Contents (Cont)

FOREWORD

This is one of a set of seven reports, each one describing the results, for a particular subsystem, of a study titled "An Engineering Study of Onboard Checkout Techniques." Under the general title of "A Guide to Onboard Checkout," the reports are as follows.

Volume	IBM Number	Subsystem
I	71W-00308	Guidance, Navigation and Control
II	71W-00309	Environmental Control and Life Support
III	71W-00310	Electrical Power
IV	71W-00311	Propulsion
V	71W-00312	Data Management
VI	71W-00313	Structures/Mechanical
VII	71W-00314	R.F. Communications

This set of guides was prepared from the results of a nine month "Engineering Study of Onboard Checkout Techniques" (NAS9-11189) performed under NASA contract by the IBM Federal Systems Division at its Space Systems facility in Huntsville, Alabama, with the support of the McDonnell Douglas Astronautics Company Western Division, Huntington Beach, California.

Technical monitor for the study was Mr. L. Marion Pringle, Jr. of the NASA Manned Spacecraft Center. The guidance and support given to the study by him and by other NASA personnel are gratefully acknowledged.

Section 1

INTRODUCTION

1.1 OBJECTIVE

With the advent of large scale aerospace systems, designers have recognized the importance of specifying and meeting design requirements additional to the classical functional and environmental requirements. These "additional" requirements include producibility, safety, reliability, quality, and maintainability. These criteria have been identified, grown into prominence, and become disciplines in their own right. Presently, it is inconceivable that any aerospace system/equipment design requirements would be formulated without consideration of these criteria.

The complexity, sophistication and duration of future manned space missions demand that still another criterion needs to be considered in the formulation of system/equipment requirements. The concept of "checkoutability" denotes the adaptability of a system, subsystem, or equipment to a controlled checkout process. As with other requirements, it should also apply from the time of early design concept formulation.

The results of "An Engineering Study of Onboard Checkout Techniques" and other studies indicate that for an extended space mission onboard checkout is mandatory and applicable to all subsystems of the space system. In order to use it effectively, "checkoutability" should be incorporated into the design of each subsystem, beginning with initial performance requirements.

Conferences with researchers, system engineers and subsystem specialists in the course of the basic Onboard Checkout Techniques Study revealed an extensive interest in the idea of autonomous onboard checkout. Designers are motivated to incorporate "checkoutability" into their subsystem designs but express a need for information and guidance that will enable them to do so efficiently.

It is the objective of this report to present the results of the basic study as they relate to one space subsystem to serve as a guide, by example, to those who in the future need to implement onboard checkout in a similar subsystem. It is not practicable to formulate a firm set of instructions or recipes, because operational requirements, which vary widely among systems, normally determine the checkout philosophy. It is suggested that the reader study this report as a basis from which to build his own approach to "checkoutability."

1.2 BASIC STUDY SUMMARY

1.2.1 STUDY OBJECTIVE

The basic study was aimed at identification and evaluation of techniques for achieving the following capabilities in the operational Space Station/Base, under control of the Data Management System (DMS), with minimal crew intervention.

- Automated failure prediction and detection
- Automated fault isolation
- Failure correction
- Onboard electronic maintenance

1.2.2 STUDY BASELINE

The study started in July 1970. The system design baseline was established by the Space Station Phase B study results as achieved by the McDonnell-Douglas/ IBM team, modified in accordance with technical direction from NASA-MSC. The overall system configuration was the 33-foot diameter, four-deck, 12-man station. Individual subsystem baseline descriptions are given in their respective "Guide to Onboard Checkout" reports.

1.2.3 STUDY TASKS

The basic study comprised five tasks. Primary emphasis was given to Task 1, Requirements Analysis and Concepts. This task established subsystem baseline descriptions and then analyzed them to determine their reliability/maintainability characteristics (criticality, failure modes and effects, maintenance concepts and line replaceable unit (LRU) definitions), checkout strategies, test definitions, and definitions of stimuli and measurements. After software preliminary designs were available, an analysis of checkout requirements on the DMS was performed.

A software task was performed to determine the software requirements dictated by the results of Task 1.

Task 3 was a study of onboard electronic maintenance requirements and recommendations of concepts to satisfy them. Supporting research and technology tasks leading to an onboard maintenance capability were identified. The study implementation plan and recommendations for implementing results of the study were developed in Task 4. The task final report also summarizes results of the study in all technical tasks.

Reliability, Task 5, was very limited in scope, resulting in an analysis of failure modes and effects in three Space Station subsystems, GN&C, DMS (computer group) and RF communications.

1.2.4 PREVIOUS REPORTS

Results of the basic study were reported by task in the following reports, under the general title of "An Engineering Study of Onboard Checkout Techniques, Final Report."

IBM Number	Title
71W-00111	Task 1: Requirements Analysis and Concepts
71W-00112	Task 2: Software
71W-00113	Task 3: Onboard Maintenance
71W-00114	Task 4: Summary and Recommendations
71W-00115	Task 5: Subsystem Level Failure Modes and Effects

Section 2

BASELINE SUBSYSTEM DESCRIPTIONS

2.1 GENERAL

This section describes the baseline Environmental Control and Life Support (EC/LS) subsystem which was analyzed to define onboard checkout requirements. In order to assess requirements for onboard checkout, descriptions at the subsystem level and the assembly level are required, as well as the major interfaces between subsystems.

The assembly level description for each of the subsystems (MSFC-DRL-160, Line Item 13) provided the primary working document for subsystem analysis. To reduce documentation, these documents have been incorporated by reference into this report where applicable. Therefore, where no significant differences exist from the Phase B definition, this report contains a brief subsystem description and an identification of the referenced document containing the assembly level descriptions for the subsystem. Where significant differences do exist, the subsystem level description includes these changes in as much detail as is available. MSFC-DRL-160, Line Item 19, provided the major subsystem interface descriptions for analysis of integrated test requirements.

2.2 SUBSYSTEM LEVEL DESCRIPTION

The EC/LS Subsystem provides cabin atmosphere control and purification, water and waste management, pressure suit support, and thermal control for the entire Space Station.

The atmosphere is nearly that at sea level; however, in accordance with the guidelines and constraints, the system is designed to operate in a variable atmosphere of 10.0 to 14.7 psi, with a partial pressure of oxygen constant at 3.1 psi, regardless of the total pressure.

Two 12-man subsystems are provided, one for the compartment (defined as a volume of space enclosed by pressure-resistant structure) which includes decks 1 and 2, and one for the compartment that includes decks 3 and 4. The tunnel can be referenced to either subsystem.

The subsystem provided has full H_2O recovery; that is, more water is recovered in the Space Station than is required for drinking and washing. The subsystem also has partial O_2 recovery; the shortage is made up by water contained in the food.

The EC/LS Subsystem provides methane and unreacted CO_2 to the Propulsion Subsystem which uses these gases as propellants for orbitkeeping and control-moment gyro desaturation.

The total heat generated in the Space Station is rejected to space through a segmented radiator integrated with the micrometeoroid shield independently of the heat distribution between compartments.

The assemblies provided in decks 1-2 and decks 3-4 each have the capability to support 12 men. The tunnel atmosphere can be interchanged with either system through the valving and interconnecting ducting; however, the atmosphere for decks 1-2 and that for decks 3-4 are not intermixed normally through the ventilation system. Cross-linking between assemblies is provided, however, to allow one assembly to serve as an installed spare for the other.

If a major emergency occurs, such as a fire, decompression, or massive contamination, it will affect only the atmosphere in half of the Space Station. The crew will always be able to live in the other compartment within the time limit established by the amount of consumables on board at the time of the emergency. This concept also easily accommodates the 24-man crew during the overlap period. The thermal control circuits are also designed to be completely independent so that if fire disables the heat-transport loops in either compartment, it does not affect the entire Space Station.

Cooling and heating requirements are satisfied independently for each of the Space Station common modules and to minimize the probability of a full loss of the Thermal Control System. However, controls are also provided whereby these heating and cooling loads may be accommodated independently of their distribution between common modules. As a limit, either common module system can accommodate full crew and electrical loads. Because all critical electrical equipment is duplicated within the two common modules, thermal control capability is essentially duplicated. One limitation is that total available radiator area is necessary to reject total cooling loads under design environmental conditions. For this reason and because radiator failures may be difficult to repair, full redundancy is provided in the radiator circuitry. Segmentation and circuit isolation further protect against major Thermal Control System loss.

2.3 ASSEMBLY LEVEL DESCRIPTIONS

Descriptions of the EC/LS Subsystem assemblies are provided in the Space Station MSFC-DRL-160, Line Item 13, Volume I, Book 3, Crew Systems. These descriptions include block diagrams, discussions of assembly groups, assemblies, and major subassemblies, physical characteristics summary, and interface descriptions. DRL 13, Volume I, Book 2, is incorporated by reference into this report as a detailed description of the EC/LS Subsystem assembly group, assemblies, and major subassemblies will become the primary working document for further analysis.

Section 3

RELIABILITY AND MAINTAINABILITY ANALYSES

3.1 CRITICALITY ANALYSIS

As a guide to emphasis in subsequent checkout technique studies, an analysis has been made of the overall subsystem and major component criticality (failure probability) of the Space Station subsystems and equipment. As an input to the Checkout Requirements Analysis Task, this data along with the failure mode and effects data will be useful in determining test priorities and test scheduling. Additionally, this data will aid in optimizing checkout system design to ensure that confidence of failure detection is increased in proportion to added system complexity and cost.

3.1.1 CRITICALITY ANALYSIS PROCEDURE

A criticality number (related to failure probability) was generated for each major subsystem component. This number is the product of: (1) the component failure rate (or the reciprocal of mean-time-between-failure), (2) the component's anticipated usage or duty cycle, and (3) an orbital time period of six months, or 4,380 hours. Six months was chosen as the time period of interest to allow one missed resupply on the basis of normal resupply occurring at three-month intervals. The criticality number, then, is the failure expectation for a particular component over any six-month time period.

For visibility, the major components of each subsystem analyzed have been ordered according to the magnitude of their criticality numbers. This number, however, should not be considered as an indication of the real risk involved, since it does not take into account such factors as redundant components, subsystem maintainability, and the alternate operational procedures available.

Overall subsystem criticality has been determined by a computerized optimization process whereby spares and redundancy are considered in terms of a trade-off between increased reliability and weight. This determination, therefore, reflects not only the failure probability of subsystem components, but also the probability that a spare or redundant component may not be available to restore the subsystem to operational status. The methodology used is described in Section 9, Long-Life Assurance Study Results, DRL 13 (Preliminary Subsystem Design Data), Volume III (Supporting Analyses), Book 4 (Safety/Long Life/Test Philosophy) from the MDAC Phase B Space Station Study. Component-level failure mode and criticality data are presented in subsequent paragraphs.

3.1.2 SUBSYSTEM CRITICALITY DATA

The Environmental Control and Life Support Subsystem (EC/LS) has a six-month reliability of 0.997 and requires 1,780 pounds of spares for its achievement. An ordered ranking of EC/LS component criticality is provided in Table 3-1.

Two completely independent EC/LS subsystems exist onboard the Space Station, either of which is capable of supporting the crewmen for extended periods of time. Table 3-1 ranks EC/LS components in an artificial worst case environment reflecting nonexistence of any backup system, but also provides conditional criticalities assuming the availability to both the backup subsystem and spares.

3.2 FAILURE EFFECTS ANALYSIS (FEA)

Based upon the baseline subsystem descriptions, each major subsystem component was assessed to determine its most probable failure mode(s), and the "mission effect" associated with this failure mode(s). The "mission effect" is noted to provide a brief explanation of Space Station behavior if the particular failure mode should occur (e.g., experiments degraded, crew hazard, etc.). The explanation generally does not, however, consider the offsetting effects of backup redundancy or spares since there would be practically "no effect" if these factors were considered.

In addition, the effect of failure is categorized into the following criticality classes:

(a) Category I - Failure could cause a loss of life.

(b) Category II - Failure could cause the loss of a primary mission objective.

(c) Category III - Failure could cause the loss of a secondary mission objective.

(d) Category IV - Failure results in only a nuisance.

In most cases, Category II and Category III failures are not distinguishable because primary and secondary mission objectives have not been identified to the level of detail required to permit such separation.

Two completely independent EC/LS subsystems exist on board the Space Station, either of which is capable of supporting the crewmen for extended periods of time. The number of units indicated in Table 3-2 (a partial listing included only to serve as an example) shows the total quantity of components utilized in both EC/LS subsystems (not including spares). The mission-effects noted in Table 3-2 reflect the non-existence of any backup subsystem and therefore depict artificial worst case conditions.

Table 3-1. EC/LS Criticality Ranking (Highest 25 Components)

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
2590 Electrolysis Module	675,000	150	includes 6 spares
6304 Pump/Motor	146,000	73	
6604 Pump/Motor	146,000	73	
6104 Pump/Motor	146,000	73	
2341 CO_2 Compressor	86,000	750	
1302 Pressure Control	83,000	100	
2231 Fan	47,500	100	
2242 Fan	47,500		
2241 Fan	47,500		
2140 Fan	47,500		
2340 Fan	47,500		
2642 Fan	47,500		

Table 3-1. EC/LS Criticality Ranking (Highest 25 Components) (Continued)

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
2370 Valve, Sequence Controller	43,800	10	
2302 CO_2 Diverter Valve	43,800	10	
2304 Silica Gel Diverter Valve	43,800	10	
3205 Mal Sieve Diverter Valve	43,800	10	
3370 Control	43,600	10	
3314 Valve, Temp Control	40,000	7	
2141 Water Pump	37,000	105	
3340 Pump	37,000	105	
2440 Condensate Pump	36,800	105	
2571 Current Controller	32,000	44	
1805 Rotating Compressor	26,200	200	

Table 3-2. Environmental Control and Life Support

	Prior Subsystem Component	Failure Mode(s)	Mission Effect	Failure Category	No. of Units	(A) MTBF/Source Thousands of Hours	(B) Duty Cycle (%)	Criticality Unit (4380 hrs x B/A x 10^{-6})
1101-1	Tank, O_2 Gas Storage	Rupture, Leakage	Loss of O_2 for compartment repressurization, airlock makeup and PLSS recharge	I	4	2,940	100	1,490
1102	Flow Restrictor, Gas Storage	Clog, Leakage	Same as 1101-1	II/III	4	10,000	100	438
1103	Shutoff Valve, Gas Storage	Open, Close	Fail to open, same as 1101-1	II/III	4	1,870	100	2,350
1104	Quick Disconnect, Gas Storage	Failure to Connect; Failure to Disconnect	Same as 1101-1	II/III	4	6,600	100	660
1105	Diverter Valve, Gas Storage	Failure to Actuate	Same as above if manifold fails (secondary failure)		4	1,870	100	2,350
1106	Pressure Transducer, Gas Storage		Instrumentation		4	280		
1101-2	Tank, N_2 Gas Storage	Rupture Leakage	Experiment curtailment, loss of N_2 for compartment atmosphere	I	8	2,940	100	1,490
1102	Flow Restrictor, Gas Storage	Clog, Leakage	Same as 1101-2	II/III	8	10,000	100	438
1103	Shutoff Valve, Gas Storage	Fail Open; Fail Closed	Same as 1101-2	II/III	8	1,870	100	2,350
1104	Quick Disconnect, Gas Storage	Fail to Connect; Fail to Disconnect	Same as 1101-2	II/III	8	6,600	100	660
1105	Diverter Valve, Gas Storage	Failure to Actuate	Same as 1101-2	II/III	8	1,870	100	2,350
1106	Pressure Transducer, Gas Storage		None-Instrumentation		8	280	100	

3.3 MAINTENANCE CONCEPTS

Space Station maintenance concepts, in general, are discussed in Section 7.

The Environmental Control and Life Support (EC/LS) Subsystem represents the largest maintenance workload and the greatest potential for commonality in design for maintenance. The EC/LS Subsystem will, for the most part, be maintained at the component level, such as a fan or a valve.

Consideration has been given to electrical design approaches that allow removal of electrical solenoids, transducers, etc., with complete isolation from the pneumatic and/or fluid systems. Attach fittings permit easy removal and installation of devices with minimum use of screws and bolts.

Filter elements are designed to permit exchange without releasing liquids or noxious gases. The electrolysis cell stack is designed to be repaired at a module or subassembly level. If a single membrane fails, the entire module is replaced. Tanks are replaceable and are of a size that will pass through the passageways to the logistics docking port.

Two radiator control and two radiator recirculation assemblies are installed in the forward pressurizable equipment deck and two each in the unpressurized area between Decks 2 and 3. Both of these are maintainable in a shirtsleeve environment.

Acceptable repair times are limited to 30 percent of the critical (maximum possible) downtime to maximize the probability of repair. Note that critical downtimes for the EC/LS Subsystem will be very long, generally because of the two-compartment design.

Downtime allowable includes time for recognizing and locating the problem, isolation time, replacement/repair time, delay time in initiating maintenance, recharge and/or restart time, and checkout time to determine if the system is performing correctly.

To minimize crew error, installation of replacement components or modules is planned as one-way-possible positioning. Labeling and coding should be employed liberally to aid maintenance.

System design will emphasize commonality to reduce the number and types of spares and, thus, crew training requirements.

Maintenance ends ordinarily at the component level. However, consideration will be given to possible emergency repairs below the component level by use of standard parts where feasible.

Components shall be designed to be replaceable by one man. Modules, if required, may be replaced by two men.

External (outside the vehicle) maintenance will be at a higher level than internal maintenance (i.e., module, subsystem, or system rather than component replacement).

Hazardous maintenance (atmospheric contamination) and external maintenance (radiators) will be performed in a pressure suit, and subsystems are designed to permit this kind of maintenance.

Components are isolated, removed, and replaced as follows:

- Low-Pressure Air Line - Simple clamp removal, no isolation required
- High-Pressure Gas - Manually operated, isolation valves
- Fluid Lines - Special low leakage, component bypass maintenance disconnects

Small components can be removed and replaced simultaneously, with the loss of a maximum of 0.1 cc of water, by an installation tool that pushes the replacement components into the manifold. The replacement component, in turn, pushes the failed component into an empty sleeve. Large components are replaced by using the installation tool (plug) to remove the component and plug the manifold.

All equipment deemed critical to Space Station operation is duplicated so that cooling can be provided by either core module coolant water circuit. This system redundancy, together with the large core module atmosphere volumes, generally precludes the need for rapid fault isolation and repair.

3.4 LINE REPLACEABLE UNIT ANALYSIS

General guidelines and criteria for the definition of LRUs were established and these along with the maintenance philosophies reported in Section 3.3 were used to determine at what level line maintenance would be performed. For the Space Station Subsystems (less DMS) specific justification applicable to LRU selection for the particular subsystem under examination was derived from the guidelines and these justifications are presented along with the LRU listing. The "functional LRUs" were then considered in the light of the standard electronic packaging scheme and actual LRUs were defined and listed. The method employed and the results achieved are discussed in the following sections.

3.4.1 SPACE STATION SUBSYSTEMS

The definition of Line Replaceable Units (LRUs) is keyed to repairing subsystems in an in-place configuration with the LRU being the smallest modular unit suitable for replacement. General factors considered in identifying subsystem LRUs include: (1) maintenance concepts developed and defined in Section 3.3; (2) the component-level failure rates delineated in the criticality analyses of Section 3.1; (3) the amount of crew time and skill required for fault isolation and repair; (4) resultant DMS hardware and software complexity; and (5) subsystem weight, volume, location, and interchangeability characteristics. Listings of LRUs and more specific justification for their selection follows.

A partial list of LRUs for the Environmental Control and Life Support (EC/LS) Subsystem is provided in Table 3-3 as an example. Replacement is at the component level primarily for efficiency of sparing and maintenance. It is at the component level where: (1) EC/LS elements are expected to require periodic replacement, (2) the number of EC/LS functions interrupted when maintenance is performed is acceptable, (3) only conventional tools are required, and (4) normal fabrication breakpoints exist. Lower level replacement would cause a disproportionate increase in instrumentation and in the complexity of tools and skills required. Higher level replacement would result in increased spares weight and volume due to a decrease in commonality of spares. For the EC/LS Subsystem, component-level LRUs offer a good compromise for the advantages and disadvantages of lower and higher level replacement.

Table 3-3.. Environmental Control and Life Support

LRU	Quantity	
	Required	Standby Redundant
High Pressure Gas Tank	12	
Flow Restrictor	30	
Shutoff Valve, Solenoid W Manual OR	27	
Quick Disconnect	95	
3-Way Valve, Electrically Operated	34	
Electric Heater	20	
Pressure Regulator with Relief	2	2
Pressure Control	1	1
O_2 Sensor	1	1
3-Way Valve, Pressure Actuated	1	1
Shutoff Valve, Manual	275	
Relief and Dump Valve	2	2
Low Pressure Tank	9	
Pressure Regulator	5	
Compressor	9	
Heat Exchanger, Liquid to Gas	2	
Check Valve	40	
Air Bypass Valve	2	
Fan	20	
Pump	33	7
Condensing Heat Exchanger	8	
Temperature Controller	7	
Temperature Sensor	8	
Adsorption Cannister	19	
CO_2 Sensor	8	

Section 4

OCS CHECKOUT STRATEGIES

4.1 SUBSYSTEM CHECKOUT STRATEGY

Before further requirements analysis, it is necessary to develop a checkout strategy for all Space Station subsystems to meet checkout objectives, which can be summarized as follows:

- To increase crew and equipment safety by providing an immediate indication of out-of-tolerance conditions
- To improve system availability and long-life subsystems assurancy by expediting maintenance tasks and increasing the probability that systems will function when needed
- To provide flexibility to accommodate changes and growth in both hardware and software
- To minimize development and operational risks

Specific mission or vehicle-related objectives which can be imposed upon subsystem level equipment and subsystem responsibilities include the following:

- OCS should be largely autonomous of ground control.
- Crew participation in routine checkout functions should be minimized.
- The design should be modular in both hardware and software to accommodate growth and changes.
- OCS should be integrated with, or have design commonality with, other onboard hardware or software.
- The OCS should use a standard hardware interface with equipment under test to facilitate the transfer of data and to make the system responsive to changes.
- Failures should be isolated to an LRU such that the faulty unit can be quickly removed and replaced with an operational unit.

- A Caution and Warning System should be provided to facilitate crew warning and automatic "safing" where required.

- Provisions must be included to select and transmit any part or all of the OCS test data points to the ground.

To attain these objectives via the use of an Onboard Checkout System which is integrated with the Data Management System, checkout strategies have been developed which are tailored to each Space Station subsystem.

Special emphasis has been applied to a strategy for checkout of redundant elements peculiar to each subsystem. The degree to which each of these functions is integrated into the DMS is also addressed.

4.1.1 SPACE STATION SUBSYSTEMS

Each major Space Station subsystem was examined with respect to the required checkout functions. The checkout functions associated with each subsystem are identified and analyzed as to their impact on the onboard checkout task. The functions considered are those necessary to verify operational status, detect and isolate faults, and to verify proper operation following fault correction. Specific functional requirements considered include stimulus generation, sensing, signal conditioning, limit checking, trend analysis, and fault isolation.

4.1.1.1 Environmental Control and Life Support Subsystem

The Environmental Control and Life Support Subsystem (EC/LSS) is perhaps the most critical of the onboard subsystems in that its proper operation is essential to the habitability of the Space Station and to the lives of the crew. The subsystem therefore features a high degree of reliability which is achieved through conservative design and through redundancy and backup provisions. Major elements of the subsystem are the atmosphere supply and control, atmosphere reconditioning, water management, waste management, IVA/EVA, and thermal control systems.

4.1.1.1.1 Checkout Functions

The EC/LSS is a mechanical and chemical subsystem and as such involves some rather unique checkout and fault isolation considerations. Probably the most apparent of these is the extremely wide spectrum of sensing requirements. These range from the relatively common, such as voltage, temperature, and pressure, to the uncommon which include PH factor and conductivity of water. Other significant characteristics of the subsystem from the checkout standpoint are its large size, wide physical distribution, and its complexity.

The subsystem performance parameters, (pressure, temperature, flow, quantity, etc.) are predominatly analog in nature and are associated with continuous process operations rather than events. Such parameters lend themselves well to limit checking as a means of status monitoring and fault detection, and this technique is used extensively. Some trend analysis is also utilized to evaluate performance of limited life items such as filters. Fault isolation is accomplished primarily through combinatorial analysis of operating conditions.

- Stimulus Generation - No external stimuli other than those required for operational control are required for checkout of the subsystem.

- Sensing - Detailed measurement requirements are included in the Task 1 Final Report.

- Signal Conditioning - Many sensors will impose requirements for signal conditioning to convert their outputs to a form compatible with the data acquisition equipment. The exact quantity and configuration will depend upon the type of sensors selected, but may include strain gauge and temperature probe conditioning, frequency to DC conversion, etc., plus scaling, amplification, and buffering circuitry. The required circuitry is provided as an integral part of the sensor assemblies or in associated electronics assemblies.

- Limit Checking - The EC/LSS involves a large number of fluid process functions such as temperature and pressures which must be monitored to assure the proper operation and safety of the subsystem. This requirement leads to the extensive use of a limit checking technique. The applicable limits include both absolute limits, such as those associated with safety, and operational limits which may vary in accordance with particular operating modes or conditions. Certain parameters have significant limits in both categories and therefore require a dual limit check. The variable aspect of the operational limits necessitates the capability for selectively altering the limit criteria in real time.

In terms of data processing requirements the large number of limit functions associated with the EC/LSS is offset to some extent by the relatively low rates involved. The majority of these functions are dynamically stable and are not subject to high rates of change. The sampling rate may therefore be quite low (i.e., one iteration/second or minute) even on the more critical functions which involve crew safety.

Detection of an out-of-limit condition in any of the EC/LSS parameters will lead to some form of relief or corrective action, either automatically or by the crew. The nature of the required action will in some cases be directly deducible, but more commonly must be determined through fault isolation techniques. A typical situation will involve a two-stage reaction, first to relieve the condition and then to correct it. An example is the detection of a sudden pressure decay in a freon coolant loop, indicating a possible rupture. Immediate and automatic action would be taken to isolate the loop to minimize further loss of fluid. This would be followed by automatic switchover to the alternate loop to maintain thermal conditioning. Fault isolation precedures would then be initiated to localize the problem and determine repair action.

- Trend Analysis - Trend analysis techniques will be utilized where applicable to accomplish predetection of potential failures or hazardous conditions and as an aid to the detection and diagnosis of abnormal conditions. Examples of predetection include monitoring of trace contaminants in the atmosphere to detect buildup trends and monitoring of CO_2 absorption bed moisture level to project useful life. The application of trend data to fault detection and diagnosis is illustrated by the use of nitrogen repressurization history to detect abnormal cabin repressurization rates which may be indicative of a leak in the vehicle pressure shell. Still another form of trend analysis is utilized in monitoring and forecasting consumables usage as an aid to resource management and resupply planning.

- Fault Isolation - Fault isolation will be accomplished primarily through comparison of the operating system performance parameters with predetermined limits and by combinatorial analysis of input/output measurements and related functions. Redundant element substitution will also be utilized where applicable.

4.1.1.1.2 Redundant Element Checkout

The EC/LSS features a high degree of redundancy at both the functional and LRU levels. Functional redundancy includes separate and independent forward and aft compartment atmosphere supply and control, water management, waste

management, and thermal control systems, each fully capable of supporting the 12-man crew. Crossover connections are provided between compartments to permit assemblies in either compartment to serve as spares for those in the other compartment. Lower level redundancy is provided in the form of parallel and/or series redundant storage tanks, pressure regulators, pumps, valves, filters, etc. In all cases the redundant systems/assemblies/components are isolatible by valving or switching and are capable of being operated and tested as independent elements. They therefore present no unique problems from the checkout standpoint other than the requirement that they be exercised periodically if not normally on line.

4.1.1.1.3 Integration with Data Management System

The data acquisition interface between the EC/LSS and the DMS is defined by the measurement list in the Task 1 Final Report. Signal conditioning is provided by the EC/LSS to convert the measurement sensor outputs to a standardized 0-20 mVdc, 0-5 Vdc, or 0-28 Vdc level. The DMS must provide the computation capability necessary to apply calibration coefficients and convert to engineering units. The DMS also provides the test control, sequencing, and fault isolation logic.

4.2 INTEGRATED CHECKOUT STRATEGY

This analysis identifies the integrated checkout functions associated with Space Station subsystems during the manned orbital phase of the mission. These functions are depicted in Figure 4-1 and are those required to ensure overall availability of the Space Station. Characteristic of integrated testing is the fact that the test involves subsystem interfaces, and, therefore, test objectives are associated with more than one subsystem.

4.2.1 INTEGRATED STRATEGY

Six checkout functions have been identified:

- Caution and warning
- Fault detection
- Trend analysis
- Operational status
- Periodic checkout
- Fault isolation

These functions represent a checkout strategy of continuous monitoring and periodic testing with eventual fault isolation to a line replaceable unit (LRU). Under this aspect the functions are grouped as -

CONTINUOUS MONITORING	PERIODIC TESTING	FAULT ISOLATION
• Caution and warning	• Automatic tests	• Localize to SS
• Fault detection	• Operational Verification	• Isolate to RLU
• Trend analysis		
• Operational status		

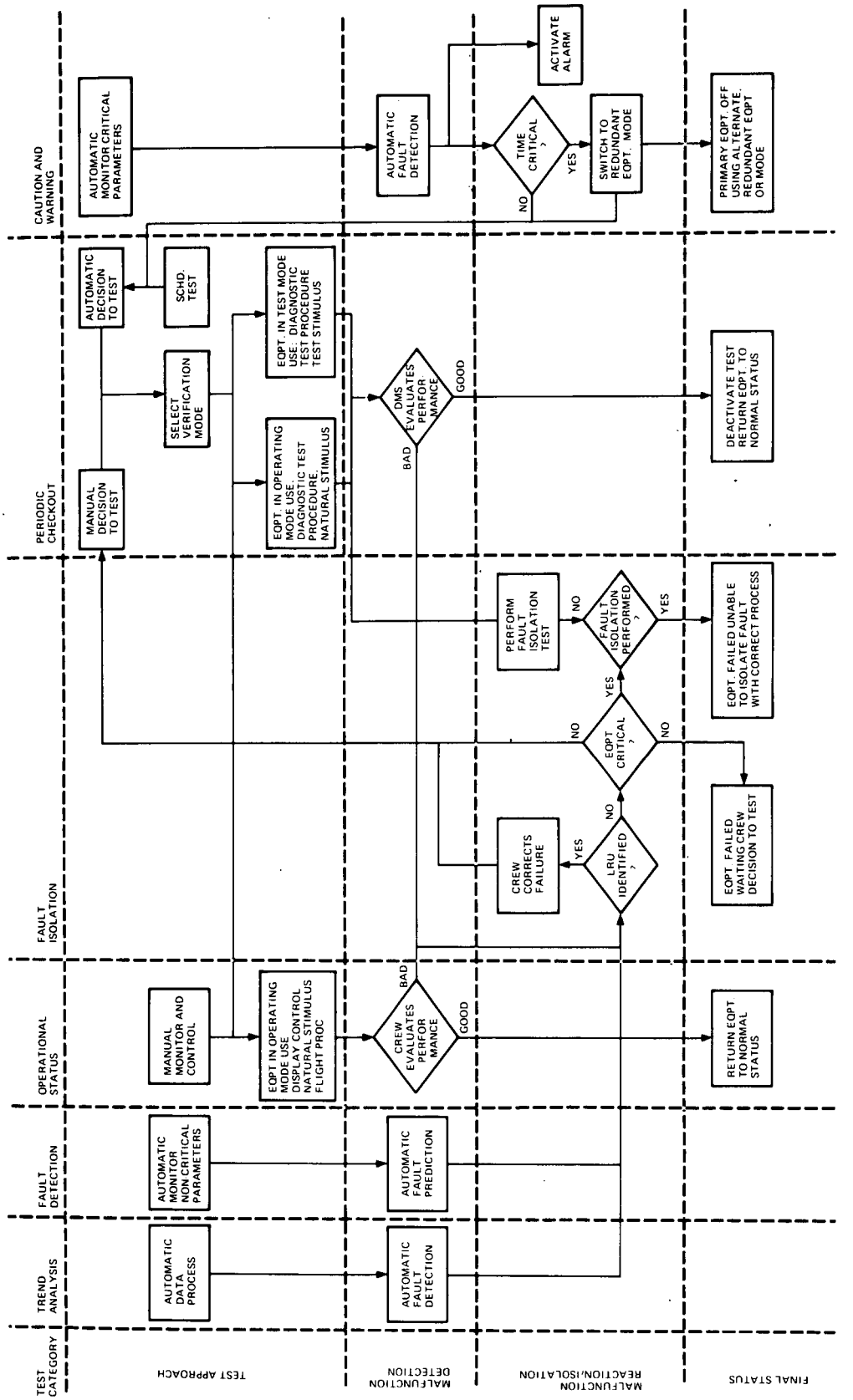

Figure 4-1. Integrated Checkout Functional Flow

General characteristics of these groups are defined below:

4.2.1.1 Continuous Monitoring

Continuous monitoring is not a test per se. It is a concept of continuously sampling and evaluating key subsystem parameters for in/out-of-tolerance conditions. This evaluation does not necessarily confirm that the subsystems have failed or are operating properly. The evaluation is only indicative of the general status of the subsystems. For example, a condition exists where the integrated subsystems are indicating in-limit conditions, but during the next series of attitude control commands, an error in Space Station position is sensed and displayed. Since three subsystems, DMS, GN&C, and P/RCS, are involved in generating and controlling the Space Station attitude, a "positional error" malfunction is not directly related to a subsystem malfunction. The malfunction indication is only indicative of an out-of-tolerance condition of an integrated function. Final resolution of the problem to a subsystem and eventually to LRU will require diagnostic test-procedures that are separate from the continuous monitoring function.

There are situations in which the parameters being monitored are intended to be directly indicative of the condition of a subsystem or an LRU. Examples of these include tank pressures, bearing temperatures, and power source voltages. However, even in these simpler cases when a malfunction is detected, an integrated evaluation will be performed to ascertain that external control functions, transducers, signal conditioning, and the DMS functions of data acquisition, transmission, and computation are performing properly. This evaluation will result in either a substantiation of the malfunction or identification of a problem external to the parameter being monitored.

Figure 4-1 shows the logic associated with each function in the continuous monitoring group, as well as the integrated relationships between these and the total checkout functions. The caution/warning and fault detection functions are alike in their automatic test and malfunction detection approaches, but are different in terms of parameter criticality and malfunction reaction. The caution/warning function monitors parameters that are indicative of conditions critical to crew or equipment safety. Parameters not meeting this criticality criteria are handled as fault detection functions. Figure 4-1 shows that in the event of a critical malfunction, automatic action is initiated to warn the crew and sequence the subsystems to a safe condition. Before this automatic action is taken, the subsystems must be evaluated to ascertain that the failure indication is not a false alarm and that the corrective action can be implemented. After the action is taken, the subsystems must be evaluated to determine that proper crew safety conditions exist. Since automatic failure detection and switching can be integral to subsystem design (self-contained correction) and subsystems can be controlled by the operational software or manual controls, it is imperative that the status of these events be maintained and that the fault detection and correction software be interfaced with the prime controlling software. For malfunctions that are not critical, the crew is notified of their occurrence, but any subsequent action is initiated manually.

The next continuous monitoring function, trend analysis, automatically acquires data and analyzes the historical pattern to determine signal drift and the need for unscheduled calibration. It also predicts faults and indicates the need for diagnostic and fault isolation activities. An example of a parameter in this category is the partial pressure of nitrogen. Nitrogen is used to establish the proper total pressure of the Space Station. Since it is an inert gas, the only make-up requirements are those demanded by leakage or airlock operation. The actual nitrogen flow rate is measured, and calculations are performed which make allowances for normal leakage and operational use. When these calculations indicate a trend toward more than anticipated use, the crew is automatically notified and testing is initiated to isolate the problem to the gas storage and control equipment or to an excessive leak path. The historical data is not only useful in predicting conditions but is also useful in providing trouble-shooting clues. The data might reveal, for example, that the makeup rate increased significantly after the use of an airlock. This could lead directly to verifying excessive seal leakage.

The final continuous monitor function is in operational status. This function is performed by the crew and is nonautomatic with the exception of the DMS computer programs associated with normal Space Station operational control and display functions. The concept of continuous monitoring recognized and takes advantage of the crew's presence and judgment in evaluating Space Station performance. In many instances the crew can discern between acceptable and unacceptable performance, and they can clearly recognize physically-damaged equipment or abnormal conditions.

4.2.1.2 Periodic Testing

As opposed to continuous monitoring, periodic testing is a detailed evaluation of how well the Space Station subsystems are performing. Figure 4-1 shows that periodic testing is not accomplished by any one technique. Rather, a combination of operational and automatic test approaches is employed. The actual operational use of equipment is often the best check of the performance of that equipment. Operation of Space Station equipment and use of the normal operating controls and displays will be used in detecting faults and degradation in the subsystems. This mode of testing is primarily limited to that equipment whose performance characteristics are easily discernible, such as for motors, lighting circuits, and alarm functions.

Automatic testing is performed in two basic modes:

- With the subsystems in an operating mode, the DMS executes a diagnostic test procedure which verifies that integrated Space Station functions

are being properly performed under normal interface conditions in response to natural or designed stimulation. This mode of testing allows the evaluation of Space Station performance without interrupting mission operations.

- For those situations where the integrated performance or interface compatibility between subsystems cannot be determined without known references or control conditions, the DMS will execute a diagnostic procedure in a test mode. In this mode, control, reference, or bias signals will be switched in or superimposed on the subsystems to allow an exact determination of their performance or localization of problem between the interfaces. Since the test mode may temporarily inhibit normal operations, the DMS must interleave the test and operational software to maintain the Space Station in a known and safe configuration.

The scheduled automatic tests are performed to verify availability or proper configuration of "on-line" subsystems, redundant equipment, and alternate modes.

- Periodic Verification of "On-Line" Subsystems - The first checkout requirement is a periodic verification that on-line subsystems are operating within acceptable performance margins. The acceptable criteria for this evaluation is based on subsystem parameter limits and characteristics exhibited during Space Station factory acceptance or pre-flight testing. The rejection criteria and subsequent decision to repair or reconfigure subsystems is based on the criticality of the failure mode. If the subsystems appear to be operating properly, but the test clearly indicates an out-of-tolerance condition, then one of the following alternatives must be implemented:

  - If the failure mode is critical, the crew normally takes immediate action to isolate and clear the problem.

  - If the failure mode is not critical, the crew can take immediate action, schedule the work at a later time, or wait until the condition degrades to an unacceptable level.

- Redundant Equipment Verification - A second checkout requirement is verifying that standby, off-line, or redundant equipment and associated control and switching mechanisms are operable. The acceptable/rejection criteria for these evaluations is identical to those for normally operating equipment. A primary distinction of this function is that equipment may have known failures from previous usage or tests. This situation occurs when the crew has knowledge of a failure but has not elected to perform the necessary corrective action. The checkout

function then becomes one of equipment status accounting and maintenance/repair scheduling. The status information is interlocked with mission procedures and software to preclude activation of failed units while they are being repaired or until proper operation following repair is verified.

- Alternate Mode Verification - The third checkout function is verifying the availability of alternate modes of operation. This function is essentially a confidence check of the compatibility of subsystems'interaction and performance during and after a change in the operating mode. To some extent this function overlaps with redundant equipment verification, but is broader in scope in that it verifies other system-operating characteristics. For example, some modes will involve manual override or control of automatic functions or automatic power-down sequences.

4.2.1.3 Fault Isolation

Fault isolation to an LRU is a Space Station goal. As shown in Figure 4-1, fault isolation testing is initiated when malfunction indications cannot be directly related to a failed LRU. The integrated test functions associated with fault isolation are localizing a malfunction to a subsystem or to an explicit interface between two subsystems and identifying the subroutine test necessary for LRU isolation. In structuring this relationship between integrated subsystem tests for fault localization and subroutine tests for fault isolation, the DMS, in conjunction with the test procedure documentation, must establish an effective man-machine interface so that in the event of an unsolved malfunction the crew will be able to help evaluate the condition and determine other test sequences necessary to isolate the problem. To accomplish this requirement, the DMS must be capable of displaying test parameters and instructions in engineering units and language and be capable of referencing these outputs to applicable documentation or programs that correlate test results to corrective action required by the crew.

Section 5

ONBOARD CHECKOUT TEST DEFINITIONS

5.1 SUBSYSTEM TEST DEFINITIONS

The on-orbit tests required to insure the availability of the Space Station subsystems are defined herein. Also delineated are the measurement and stimulus parameters required to perform these tests. Two discrete levels of testing are defined, i.e., continuous status monitoring tests for fault detection of critical and noncritical parameters, and subsystem fault isolation tests for localization of faults to a specific Line Replaceable Unit. In addition to these two levels, tests are defined for periodic checkout and calibration of certain units, and parameters requiring analysis of trends are defined.

The software module approach to DMS checkout makes it necessary to estimate the CPU time and memory required to implement these modules, along with an assessment of the services required from an Executive Software System to control the checkout.

These test descriptions, measurements, and stimulus information provided for each subsystem, and the software sizing information provided for the Data Management System provide the data required to estimate the checkout impact on the DMS software and hardware. Table 5-1 is a summary of the measurement and stimulus requirements for the Space Station.

The Environmental Control and Life Support (EC/LS) Subsystem provides the atmosphere supply and control, atmosphere reconditioning water management, waste management, and thermal control functions for the Space Station, including the IVA/EVA Systems. Proper operation of the subsystem is essential to the habitability of the Space Station and to the lives of the crew. The subsystem therefore features a high degree of reliability which is achieved through provision of redundancy and backup operating modes.

The EC/LS Subsystem normally operates in an automatic closed-loop mode under overall supervision of the Data Management System (DMS). An important function of the DMS will be to maintain a vehicle mass balance to project expendables use rates and to identify equipment which is not reclaiming oxygen and water at the required efficiency. The measurement/stimulus list for the EC/LS is given in the Task 1 Final Report.

Table 5-1. Measurement/Stimulus Summary

SUBSYSTEM	STIMULUS					RESPONSE				STATUS MONITORING							
	Analog	Bilevel	Digital	Pulse	RF	Analog	Bilevel	Digital	Total	Non-Critical	Caution	Warning	Periodic Checkout	Calibration	Trend	Fault Isolation	Remarks
Guidance, Navigation and Control	20	145	62	6		127	161	70	692	130	16		516	74	74	592	
Propulsion-Low Thrust		134				120	124		378	152	14		378	48	8	378	
Propulsion-High Thrust		126/62				287/117	123/63		536/242	80/28	33/15	14/10	536/242	259/111	117/43	482/222	Arc-g/Zero-a periods
Environmental Control/ Life Support	12	111				683	294		1100	147	209	32	1100		135	1100	172 Caution/Warning Signals are for IVA/EVA
RF Communications	37	206	36		77	131	286	28	801	58			576	24	93	801	
Structures	13 11	115/13				49/42	69/50		196/126	7			103/84			146/126	
Electrical Power-ICD	71	367				523	454		1415	520	18		993		143	1415	
Electrical Power-I BR	6	2				132	48		188	2	28	8	32		17	176	
Data Management			53			33	188	83	357	357			62	62	62	357	
Total	157 155	1107/1041	151	6	77	2085/1908	1747/1678	181	5511/5299	1755/1401	318/300	54/50	4296/3983	467/319	549/575	5415/5165	

5.1.1 STATUS MONITORING

Status monitoring instrumentation is provided for major parameters which reflect performance and operational status of the subsystem. Any appreciable degradation of subsystem performance is detected by limit checking. Depending upon the nature of the fault the crew receives a normal malfunction notification or a caution or warning alarm. Caution pertains to a condition of station degradation where some station activities may be curtailed. A warning is given when life critical systems are involved and the crew is in immediate danger.

Fault detection acceptance or rejection criteria are based on historically or analytically derived definitions of normal operation. Each individual fault detection parameter must be considered separately and acceptance or rejection criteria selected which accurately reflect performance. Limits on acceptance criteria are made sufficiently broad to avoid premature or erroneous fault warnings, yet with adequate margin to avoid the development of hazardous conditions.

Normally, not all the EC/LS equipment is operating at a given time and an inventory of on-line assemblies must be kept by the DMS. This inventory is required to condition limit checking and other fault detection procedures so as to prevent false malfunction warnings for shutdown equipment. Also, EC/LS assemblies which operate in a cyclic mode possess parameters which vary greatly over the cycle. Provisions must therefore be made for conditioning the tests of these parameters with the normal for that point in the cycle.

5.1.2 TREND ANALYSIS

Trend analysis is utilized for functions which are subject to performance degradation of known and measurable characteristics. These include electrolysis cells, reverse osmosis membranes, adsorption beds, and evaporator wicks. By observing the change in the major performance parameters, component replacement can be scheduled at a convenient time for the crew. Hazardous conditions can be avoided by trend analysis prediction of out-of-tolerance conditions. Trend analysis is also used to monitor expendable use rates. This pinpoints locations of excessive expendables use rates indicative of possible leakage or other failures, and also provides a basis for resources management and resupply planning activities. An example of this application is the use of nitrogen repressurization history to detect abnormal cabin repressurization rates which may be indicative of a leak in the vehicle pressure shell.

5.1.3 PERIODIC CHECKOUT

The EC/LS is periodically checked out to determine its status at specific periods in the mission. Checkout just prior to resupply is advantageous so that any deficiencies can be identified and replacements can be included in the resupply provisions.

The general checkout sequence addresses the least dependent functional group first. As an example, the thermal control equipment is checked out first because its operation does not depend on other functional groups. However, many other assemblies depend upon proper operations of the thermal control equipment. By verifying thermal control, deficiencies due to inadequate heating and cooling are eliminated as possible causes of deficiencies in EC/LS equipment. The sequence for checkout of functional groups follows the sequence below.

1. Thermal Control
2. Atmosphere Supply
3. Atmosphere Reconditioning
4. Water Management
5. Waste Management
6. IVA/EVA

Sequencing within an assembly group follows the same general procedure; the assemblies and LRUs which are least dependent are checked first. Where applicable, test sequencing is established by combinational analysis requirements.

Only a portion of the LRUs will be operating at a given time during the mission. Therefore, in order to accomplish checkout, stimuli will be provided by the DMS to exercise the EC/LS.

Units on standby redundancy are checked out by switching operation from the normally operating unit.

Acceptance or rejection criteria will consist of detecting on-off type components which fail to operate or detecting equipment which falls short of qualitative performance requirements. In some cases, on-off equipment is tested for performance as well as actuation. An example is a shut-off valve which is tested for actuation and for leakage. Leakage beyond allowable tolerance results in degraded subsystem performance and is considered a fault. Tolerance bands are chosen sufficiently broad to avoid premature fault identification and high utilization of spares. In many cases, some performance degradation can be tolerated in order to extract more life from components.

5.1.4 FAULT ISOLATION

Once the fault detection function has identified an abnormality in the EC/LS, tests are performed to identify the failure down to the LRU level. This entire procedure can be performed by the DMS in nearly all cases. A major exception is fluid and gas lines, where the exact location of a failure such as a blockage or leak cannot in some cases be performed by inplace instrumentation. Portable instrumentation and visual inspection procedures adapt readily to this application.

Fault isolation functions utilize much of the procedure software which is used for the periodic checkout function. The major difference is that the fault detection process has generally narrowed the failure location down to a small portion of the EC/LS. The point of entry into the functional test procedure is therefore determined by the malfunction indicated, and only that portion of the test necessary to identify the failed LRU is executed. Following repair or replacement, proper operation is verified by retesting.

Another valuable fault isolation tool is the onboard crew member. His powers of observation and reasoning in some cases enable him to detect and isolate faults which may elude the efforts of an automated system or which are difficult to detect by instrumentation, as in the case of fluid leakage. Planned utilization of the crew for routine fault isolation will be minimized, however, due to the limitations on available manpower resources.

A typical fault isolation flow is illustrated in Figure 5-1. This flow is initiated upon detection of excessive CO_2 in the cabin atmosphere and proceeds to isolate the fault to the appropriate LRU or to determine the required corrective action.

5.2 INTEGRATED TEST DEFINITION

The task of ensuring overall Space Station availability is primarily dependent upon the proper structuring of individual subsystem tests. The ability to test the subsystems independent of other subsystems is directly related to the number and types of interfaces. As shown in Figure 5-2, the DMS and Electrical Power Subsystems (EPS) interface with every other Space Station subsystem. In addition, the EC/LS Subsystem provides cooling to most of the electronic packages.

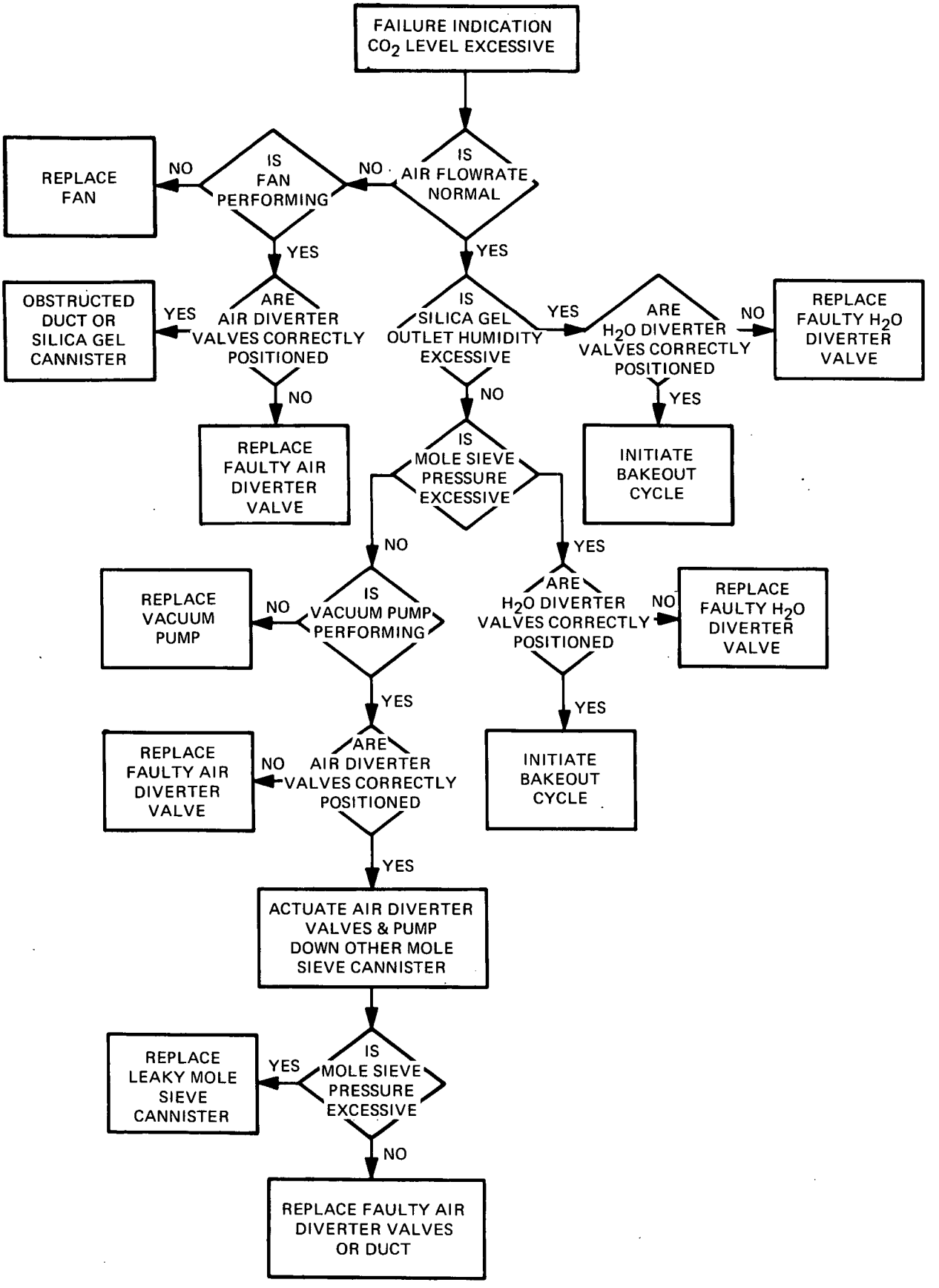

Figure 5-1. Logic Diagram for CO_2 Concentration Fault Isolation

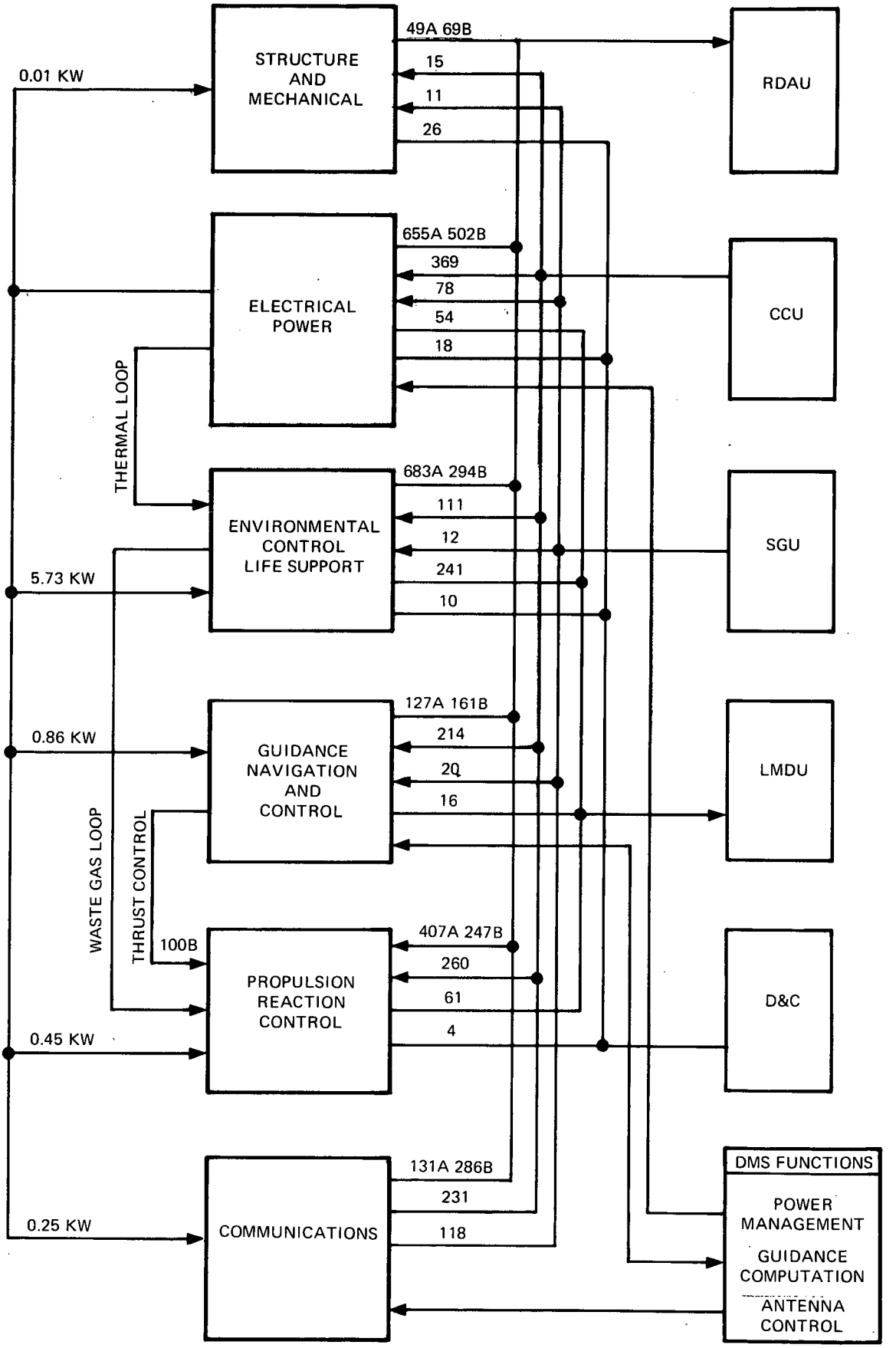

Figure 5-2. Subsystem Interfaces

This situation demands that in constructing the test for a subsystem these interfaces be taken into account so that erroneous or ambiguous test results will not be obtained. In other words, before detailed subsystem fault isolation tests are initiated, a higher level of testing should be performed to verify that all interfaces and Space Station conditions that influence the subsystem are proper. Properly designed, these higher-level tests will (1) indicate what Space Station conditions must be verified, maintained, or changed; (2) localize the malfunction to a single subsystem; and (3) identify the subroutine test necessary for fault isolation.

Since the DMS interfaces with all of the Space Station subsystems and is used as the OCS, it would appear that all of the tests would be integrated. However, this is not a proper interpretation. When the DMS is used to verify the performance of another subsystem, it must first establish itself as a test standard against which the subsystem parameters are compared. Subsequent to this verification, the test is dedicated to the evaluation of the subsystem. This test would be considered as an independent test since the objective of the test was to verify the subsystem and not the DMS. For a test to be considered as an integrated test it must meet one or more of the following conditions:

- Test objectives associated with more than one subsystem
- Test involves subsystem interfaces
- Test requires proper operation of other subsystems

In several cases, the DMS must simultaneously perform the dual role of OCS and functional elements. As an example, the DMS has a functional interface with the GN&C and Prop Subsystems for the computation of guidance equations and the execution of commands to the control actuators. When this functional closed loop is being tested, the DMS must, in addition to performing its normal functions, execute the test routine. For this type of integrated test there must be an intrinsic relationship between the operational and test software. This relationship must be carefully considered in structuring the integrated tests since unstable or intermittent performance may be detected only in the exact operating mode under closed-loop conditions. The number of integrated tests is not extensive due to the approach of minimizing the different types of interfaces between Space Station subsystems. For example, interfaces between the DMS and other subsystems are largely standardized. As a result, relatively common tests can be designed for verification of the multitude of DMS subsystem interfaces or for localization of a fault to one side of a DMS subsystem interface. All special integrated tests that have been identified are discussed in the following paragraphs. The GN&C/DMS/PROP configuration for navigation and attitude control poses the most difficult problem for on-orbit testing so it is presented in significant detail. Other integrated tests are summarized.

5.2.1 EC/LS - EPS ISOTOPE/BRAYTON INTERFACE

The Environmental Control/Life Support (EC/LS) Subsystem interfaces with the EPS Isotope/Brayton System for removal of waste heat via a fluid heat exchanger installed in the Brayton Power Conversion System. It is planned that flow rate, temperature, and pressure parameters be continuously monitored on both sides of the interface as part of normal EPS and EC/LS Subsystem checks.

5.2.2 EC/LS - LOW-THRUST PROPULSION INTERFACES

The EC/LS Subsystem interfaces the low-thrust portion of the Propulsion Subsystem to supply unreacted CO_2 from the CO_2 removal assembly, methane by-products from the CO_2 conversion assembly, and excess water. The Propulsion Subsystem uses these biowaste fluids in the Low-Thrust System as propellant. The interface is controlled by the DMS or by manual control to satisfy such parameters as propellant and pressurant selection. These parameters are primarily a function of impulse requirements and available stores. Checkout of the interface is required to verify proper valve and pump operation for the transfer of the waste gases and excess water.

Section 6

SOFTWARE

6.1 GENERAL CONSIDERATIONS

The recommended software checkout startegy involves a sequence of detecting faults, isolating faults to a failing LRU or LRUs, and reconfiguring the system to continue operation while the failures are being repaired.

This recommendation was developed by evaluating each subsystem with respect to the three general requirements of fault detection, fault isolation, and reconfiguration.

Fault detection incorporates both the recognition of failure occurrence, and the prediction of when a failure can be expected to occur. The Remote Data Acquisition Units (RDAUs) continually check selected test point measurements against upper and lower limits, and notify the executive on an exception basis when a limit is exceeded. This approach avoids occupying the central multi-processor with the low-information task of verifying that measurements are within limits.

Trend analysis is a fault detection technique recommended for predicting the time frame during which a failure can be anticipated. Data is acquired on a basis of time or utilization, and compared with previous history to determine if a "trend" toward degraded performance or impending failure can be detected.

Another checkout requirement evaluated for each subsystem is periodic testing. This type of test is provided to exercise specific components at extended time intervals or prior to specific events, to assure operational integrity. In the event that a failure is detected, the periodic test will isolate to the failing Line Replaceable Unit (LRU) and accomplish recertification after a repair operation.

Calibration of specific subsystem components will be required periodically, or subsequent to a repair and/or replace operation. The techniques involved are unique to the individual component; and, in some cases, require the acquisition of operational data.

Fault isolation is required when a fault is detected. When a particular fault provides an indication that a life critical failure has occurred, the fault isolation routines are automatically initiated. If the failure does not represent an immediate danger to the vehicle occupants, the crew is notified and they will initiate the fault isolation modules at their convenience.

The basic requirements of the fault isolation function is to analyze the available information relevant to a problem, and identify the LRU which is responsible for the anomaly.

Three basic approaches to meeting this requirement were considered. These are:

- Analyze each fault as an independent problem
- Analyze each fault with a state matrix which defines the possible error states of the subsystem
- Associate each fault with a specific subsystem, and evaluate that subsystem in detail

The third approach was selected on a basis of software commonality and cost effectiveness. The complexity associated with the testing can be reduced by localization of the logic associated with the analysis of the subsystem in a unique package. The software commonality will result in reduced software development and maintenance costs, while increasing the reliability of the software.

The fault isolation software is structured modularly for compatibility with the hardware structure of the subsystem. Checkout modules evaluate the performance of a specific portion of the subsystem. A convenient division for this modular structure is at the assembly level or functional area. A program module which can determine and control the sequence in which these checkout modules are executed is also required for each subsystem.

Subsequent to fault detection, the software associated with the subsystem which is most likely to contain the error will be activated.

The subsystem software will analyze the error indication, and initiate a sequence of checkout modules to isolate the problem. If successful, the crew is notified regarding the Line Replaceable Unit (LRU) to be replaced. If an error cannot be identified, the crew is informed of the situation and has an option to execute the periodic test of the subsystem.

After a fault has been isolated, reconfiguration software restores the functional capability of the subsystem. This is most commonly accomplished by exchanging a redundant element for the failing unit, or by defining an alternate path to accomplish the required function.

The Task 2 Final Report of the basic onboard checkout techniques study provides descriptions of the software requirements, definitions and design in addition to detailed flow charts of specific checkout routines.

6.2 SOFTWARE REQUIREMENTS

The Environmental Control/Life Support (EC/LS) Subsystem provides cabin atmosphere control and purification, water and waste management, pressure suit support, and thermal control for the entire space station.

The fault detection functions required for the EC/LS Subsystem is accomplished by tables which are monitored by the OCS executive program. The tables contain the parameters which must be monitored to assure subsystem performance. These tables are transferred to the Remote Data Acquisition Unit (RDAU) via the master executive program and exception monitoring is accomplished. Figure 6-1 provides a graphic description of this function.

Initiation of the periodic checkout function is accomplished as the result of a keyboard entry by a crew member. It is anticipated that periodic checkout will be accomplished just prior to resupply, so that required replacements can be included in the resupply provisions.

Fault isolation utilizes the same software modules as the periodic checkout; however, it is anticipated that analysis of the detected error will permit selection of the appropriate module to begin the required fault isolation. If the error is not detected in the selected assembly, the program provides this information and recommends that the periodic test be executed.

Six specific functional areas of this subsystem require automated checkout, as follows:

- Thermal Control
- Atmosphere Supply and Control
- Atmosphere Reconditioning
- Water Management
- Waste Management
- IVA/EVA

Figure 6-2 provides a block diagram of the functional areas of this subsystem.

6.2.1 SYSTEM REQUIREMENTS

6.2.1.1 Subsystem Definition

This program specification is based upon the subsystem definition given in the Task 1 Final Report. Some test points in this subsystem are currently defined

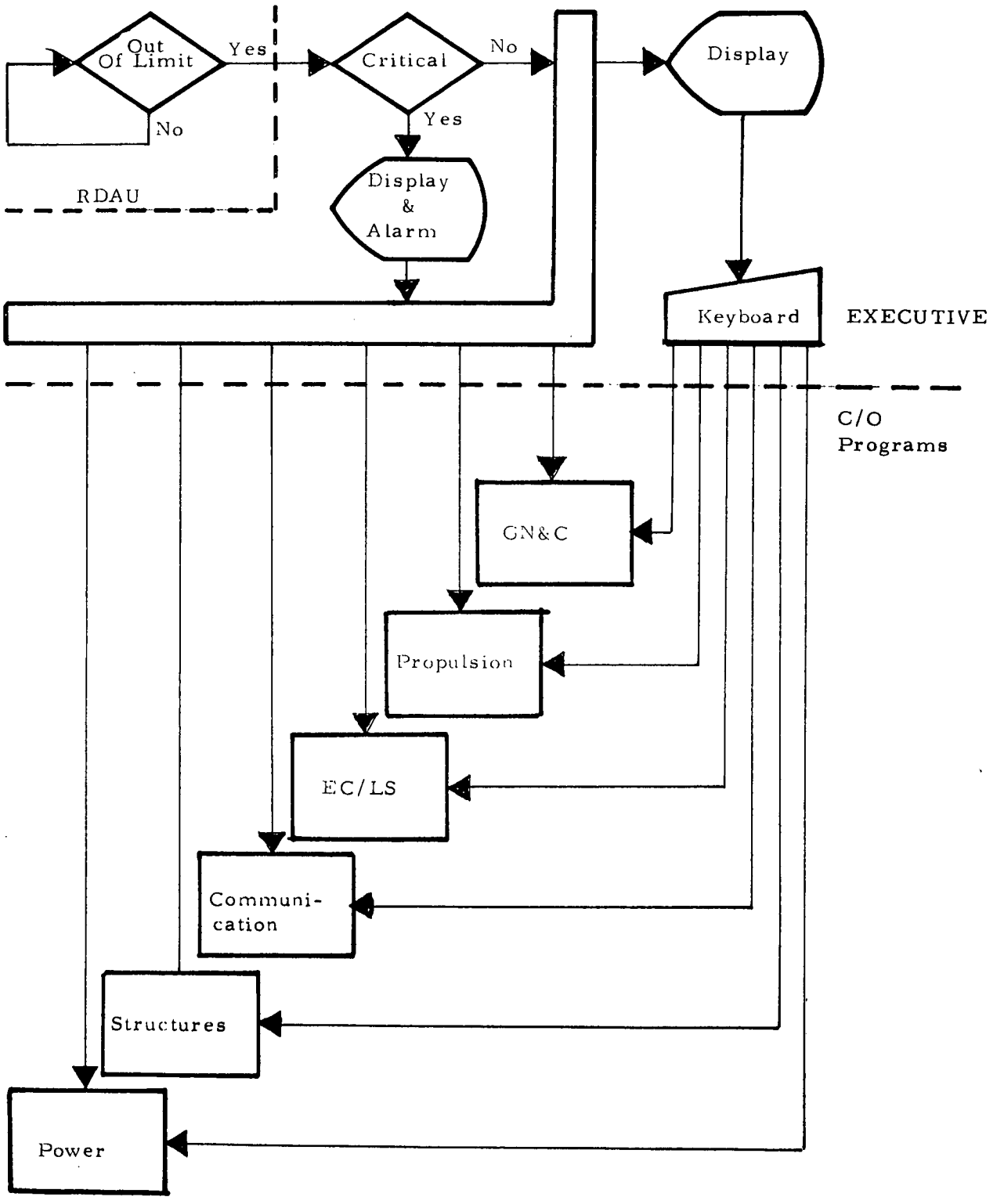

Figure 6-1. Fault Detection Logic

Table 6-1. EC/LS Fault Detection Summary

Assembly Group \ Sample Rate	1/SEC	1/MIN	1/HOUR
ATMOSPHERE SUPPLY	50		
WATER MANAGEMENT	22	8	
THERMAL CONTROL	68		
WASTE MANAGEMENT	8		
IVA/EVA SUPPORT*	120		
ATMOSPHERE RECONDITIONING	60		
PER SECOND	228		
PER MINUTE	13600	8	
PER HOUR	820,800	480	
PER DAY	20,699,200	10,520	
TOTAL PER DAY	20,709,720		

* Only during IVA/EVA Activity

at the assembly level, and consequently every failure which is detected cannot currently be identified with a Line Replaceable Unit (LRU). Also, the correlation between the assembly test points identified in the "Subsystem Test Descriptions and Measurement Stimulus List" and the LRUs identified in the "Line Replaceable Units Definition" is not always apparent.

6.2.1.2 Thermal Control Assembly Group

There are no test points defined to permit exchange of active and redundant elements under control of the computer. The existence of such test stimuli is required for execution of the periodic test.

6.2.1.3 Water Management Group

The Urine Recovery assembly in the Water Management assembly group requires a test point to open and close the solenoid valves which are associated with the chemical injector.

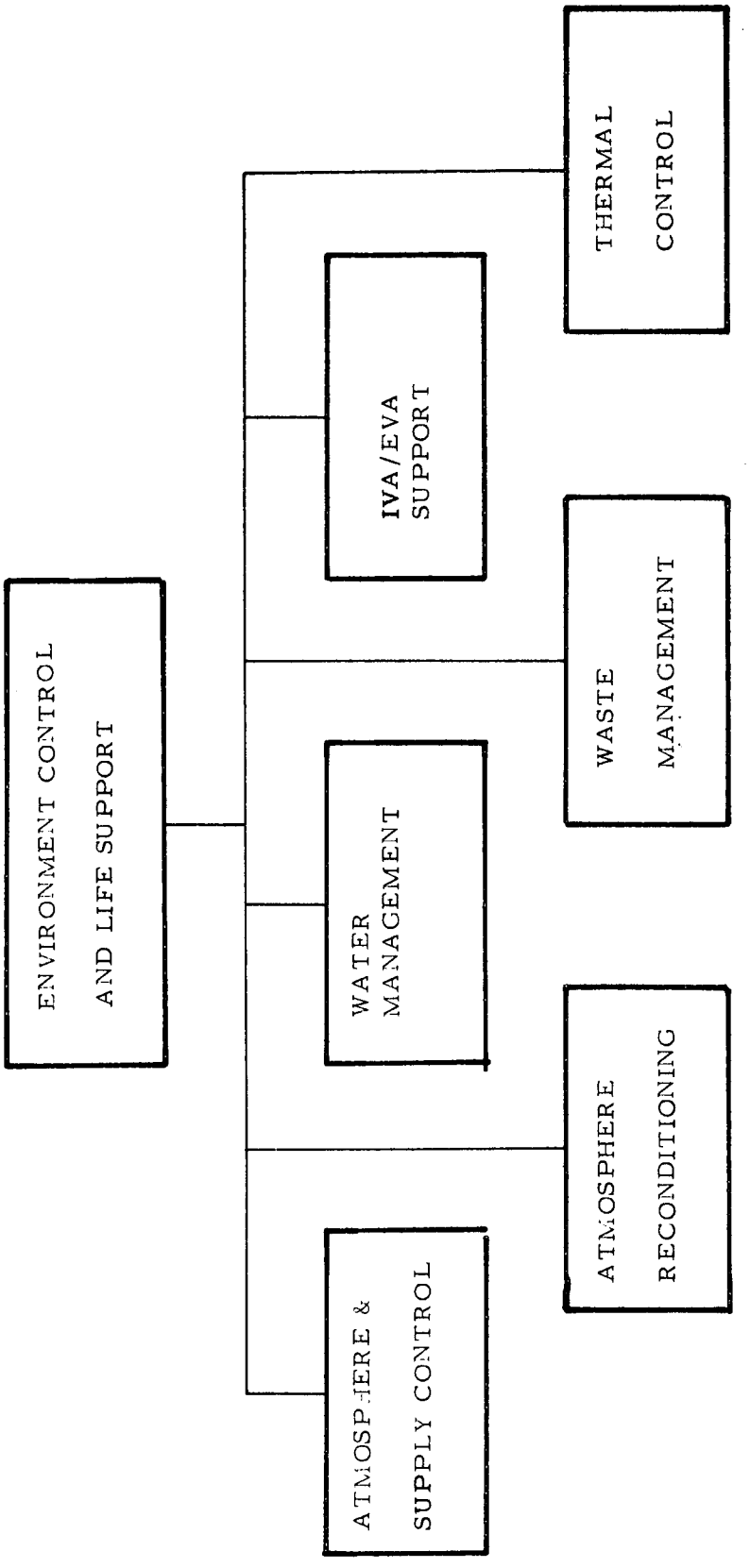

Figure 6-2. EC/LS Subsystem Functional Areas

6.2.1.4 Waste Management Assembly Group

A test point is required to determine the fecal collection seal cover position. The measurement stimulus list has been modified to omit status monitoring of the fecal container pressure.

A test point is required to provide the position of the selector valve.

A test point is also required to determine the position of the handle which indicates the operate and process phases.

6.2.1.5 IVA/EVA Assembly Group

Flowcharts were not developed for this subsystem.

6.2.1.6 Trend Analysis

Trend analysis is utilized for functions which are subject to performance degradation of known and measurable characteristics. These include electrolysis cells, reverse osmosis membranes, absorption beds, and evaporator wicks. By observing the change in the major performance parameters, component replacement can be scheduled at a convenient time for the crew. Hazardous conditions can be avoided by trend analysis prediction of out-of-tolerance conditions. Trend analysis is also used to monitor expendable use rates. This pinpoints locations of excessive expendable use rates indicative of possible leakage or other failures, and also provides a basis for resources management and resupply planning activities. An example of this application is the use of nitrogen repressurization history to detect abnormal cabin repressurization rates, which may be indicative of a leak in the vehicle pressure shell.

Although the measurement and stimulus list has identified those points which require trend analysis, the required algorithms have not been specified. Consequently, the trend analysis requirements could significantly impact the estimates which are based on a least squares technique.

Table 6-2 has been included to provide an overview of the amount of trend analysis which must be accomplished.

6.2.2 OPERATIONAL REQUIREMENTS

The general checkout sequence addresses the least dependent functional group first. The thermal control equipment is checked out first because its operation does not depend on other functional groups. Many other assemblies depend

Table 6-2. EC/LS Trend Analysis Summary

Assembly Group \ Sample Rate	1/MIN	1/HOUR	1/DAY
Atmosphere and Control	4	24	
Water Management	8	48	4
Thermal Control		8	
Waste Management			
IVA/EVA			
Atmosphere Recondition	7	32	
Data Item/Min			19
Data Item/Hour			1,252
Data Item/Day			30,052

upon thermal control equipment outputs. By verifying thermal control, deficiencies due to inadequate heating and cooling are eliminated as possible causes of problems in the EC/LS equipment. The checkout of functional groups follows the sequence below.

- Thermal Control
- Atmosphere Supply
- Atmosphere Reconditioning
- Water Management
- Waste Management
- IVA/EVA

Sequencing within an assembly group follows the same general procedure; when the assemblies and LRUs which are least dependent can be identified, they are checked first.

6.2.2.1 Thermal Control Module

The function of the thermal control assembly group is to collect, transport, distribute, and reject space station heat such that the crew and equipment are

maintained within the required temperature limits. This program module issues stimulus and monitors test points to assure the effectiveness of this operation.

The inputs to this module are the test points associated with specific assemblies. The assemblies which are examined to assure the quality of thermal operations include:

- Heating water circuit control assembly (Isotope/Brayton only)
- Heating water recirculation assembly (Isotope/Brayton only)
- Coolant water control assembly
- Coolant water recirculation assembly
- Radiator control assembly
- Radiator recirculation assembly

The outputs from this module are the normal operational messages indicating the out-of-tolerance situations and progress of the testing.

The condition of the thermal control assembly group is evaluated by software examination of the temperature and flow rates of coolant water and Freon.* If these measurements are within limits, the remainder of the tests are bypassed for purposes of fault isolation.

The periodic test performs the following tests on each assembly group in sequence.

1. The Heating Water Circuit Control Assembly controls the passage of water through the heat exchangers. This program module is capable of isolating faults which occur in the heat exchangers and relief valves.

2. The Checkout Requirements for the Heating Water Recirculation Assembly are essentially identical to those for the radiator recirculation assembly.

3. The Coolant Water Control Assembly is used to determine the required flow rate based on heat loads within the circuit. Fault isolation to the temperature sensors and the controller can be accomplished by this program module.

---

*Trademark of the DuPont Company

4. The Coolant Water Recirculation Assembly is used to maintain the flow and pressure rates within the system. The software module which checks out this assembly is capable of isolating problems in the pump and accumulator.

5. The Radiator Control Assembly includes the valves and associated controls for radiator selection and isolation purposes. The software module associated with this assembly is capable of detecting faulty operation of the isolation and flow reversal valves. There are two assemblies per module, and two complete circuits within each assembly. This configuration provides the capacity to maintain two circuits in an active state, and two circuits in a redundant status.

6. The Radiator Recirculation Assembly performs a function similar to the coolant water recirculation assembly for the Freon in the system. The basic difference is that the pump rate is not controlled by the radiator control assembly. Two additional test points have been provided to permit the sequence to check the Freon temperature and flow rates. This checkout program module is capable of isolating problems in the pump and accumulator.

Trend analysis is used to evaluate trends which are developing based upon the water and Freon temperature. The required algorithms to accomplish this analysis are currently undefined.

The replacement of the Isotope/Brayton power system with a solar array power system impacts the thermal control assembly group in that the heating water recirculation assembly and heating water control assembly are no longer included.

6.2.2.2 Atmosphere Supply and Control Module

The major functions of the atmosphere supply and control assembly groups are:

- Provide oxygen and nitrogen
- Maintain atmosphere pressure and composition control
- Provide for compartmental pressurization and depressurization

The inputs to this module are the test points associated with specific assemblies. The assemblies which are examined to assure the quality of the atmosphere supply and control assembly group performance are:

- Dump and relief valve assembly
- Oxygen gas storage assembly
- Nitrogen gas storage assembly
- Pressure reduction assembly
- Airlock pump assembly
- Pumpdown accumulator assembly
- Airlock pumpdown pressure control assembly
- Docking port pumpdown pressure control assembly

The outputs from this module are the normal operational messages indicating out-of-tolerance conditions, failing LRUs, and the progress of the listing.

The checkout of the atmosphere supply and control assembly group is accomplished by a group of program modules which meet the requirements for both periodic checkout and fault isolation. The assemblies were divided into groups of associated assemblies as depicted in Table 6-3. The pressure group is primarily responsible for maintaining cabin pressure. Two systems supply the requirements for the entire space station. The pump group interfaces with areas which require repressurization and depressurization.

The checkout of both groups is accomplished on line by allocation of specific elements.

If an error is detected in either of the areas which cannot be isolated to an assembly, the failure is assumed to have occurred in the plumbing.

This program module begins execution by checking the Dump and Relief Valve Assembly. This assembly prevents excess pressure being built up in a compartment, and provides the capability to manually purge the atmosphere. The dump and relief valve position is examined. An open status or excess pressure reading is used as an indication of a pressure problem. The program begins to examine the assemblies which are in the pressure group.

The Oxygen Gas Storage Assembly is used to store the oxygen used for the compartmental atmosphere. For fault isolation the tank pressure and temperature are limit checked and if in tolerance, the fault isolation logic proceeds to the next assembly. If a test point is detected out-of-limits or the periodic test is being executed, further analysis is performed.

Table 6-3. Atmosphere Supply and Control Assembly Grouping

Pressure Group

- Oxygen Gas Storage Assembly
- Nitrogen Gas Storage Assembly
- Pressure Reduction Assembly
- Pressure Control Assembly
- Dump and Relief Valve Assembly

Pump Group

- Airlock Pump Assembly
- Pumpdown Accumulator Assembly
- Docking Port Pumpdown Pressure Control
- Airlock Pumpdown Pressure Control

The Nitrogen Gas Storage Assembly accomplishes the same function for the nitrogen gas as the Oxygen Gas Storage Assembly performs for the oxygen. Consequently, the required software is identical to that required for the Oxygen Gas Storage Assembly.

The Pressure Reduction Assembly is used to reduce the pressure of the oxygen and nitrogen which is being taken from storage. The fault isolation portion of this module limit checks the upstream and downstream pressures for both oxygen and nitrogen. If these are within limits, this assembly is considered operational. If a test point is detected out-of-limits, or the periodic test is being executed, the shutoff valves, diverter valves, and heaters are examined.

The Pressure Control Assembly controls the supply of nitrogen to the cabin and the pressure in the tunnel. This assembly requires that gas use rates be available for display to the operator upon demand. In addition, the number of actuations which are accomplished on the solenoid valve must be maintained for purposes of trend analysis.

The pressure in the oxygen supply and cabin pressure are limit checked to assure proper operation of this assembly. If either exceed limits or if a periodic test is being conducted, the solenoid valves and cabin pressure control are also checked out.

The Airlock Pump Assembly is used to reclaim atmosphere from areas which are operationally pressurized and depressurized. This reclaimed air is then pumped to the Pumpdown Accumulator Assemblies.

The repressurization line pressure is checked for both periodic testing and fault isolation. If this test point is in limit, the fault isolation test will proceed to the next assembly. If an error is detected or the periodic test is being executed, the solenoid valves and reciprocating compressor are examined.

The Docking Port and Airlock Pumpdown Pressure Control Assemblies are used to control the rate of pressurization and depressurization of the respective areas. This program module checks each docking port and airlock. The operational software has the responsibility for assuring that the proper limits are maintained in the RDAU limit table, based upon the pressurization status of the specific areas.

The Pumpdown Accumulator Assemblies are used to store air until it is needed for repressurization. Each assembly is equipped with a shutoff valve to isolate the equipment in the event of a failure.

The periodic and fault isolation tests both check the pressure and temperature in each assembly.

Trend analysis requirements for this module indicate that the executive must collect tank temperature and pressure from the N_2 and O_2 supply tanks on an hourly basis. In addition, the executive must maintain a count of the number of solenoid valve actuations in the pressure control assembly.

6.2.2.3 Other Modules

The foregoing descriptions should suffice as examples. A more complete treatment is discussed in the Task 2 Final Report.

6.2.3 INTERFACE REQUIREMENTS

This program must interface with the master executive, the OCS Executive, and the EC/LS Subsystem hardware. The EC/LS must also interface with the following subsystems.

- Power Subsystem
- Structure Subsystem
- Propulsion Subsystem
- Data Management Subsystem

The operator is required to communicate with the program to accomplish the desired function. Specifically, the operator must initiate the program using the system communication function. The program may be terminated prior to completion by using the TERM system communication function.

In addition, when errors are detected, the operator is provided with options to control program execution sequence. These options are referred to as GO-NO GO options and permit the operator to retest the LRU which failed, resume program execution, or to terminate program execution.

The operator must be capable of identifying the IVA and umbilical which are associated with the particular pressure suits.

6.2.3.1 Interface Diagrams

The interface between the EC/LS and other subsystems is depicted in Figure 6-3. Table 6-4 reflects the interface between the EC/LS Subsystem Checkout Program and the Executive Program.

Figure 6-4 is an example of the assembly interfaces which must be considered.

6.2.3.2 Detailed Interface Definition

6.2.3.2.1 Subsystem Interfaces

Power Subsystem - The electrical power subsystem supplies power to all of the assemblies of the EC/LS subsystem requiring electrical power.

Structure Subsystem - The radiator tubes are integrated with frames of the meteoroid shield. The EC/LS subsystem interfaces with the radiator at the inlet and outlet mainfolds.

All EC/LS subsystem assemblies are mounted in the structure, and interconnecting plumbing and electrical wire harnesses are supported by the structure.

The EC/LS pumpdown system provides for pressurization and depressurization of the EVA airlock, the forward tunnel, and the equipment bay.

Propulsion Subsystem - The EC/LS subsystem supplies unreacted CO_2 from the CO_2 removal assembly to the propulsion subsystem. Excess water is also transferred to the propulsion system.

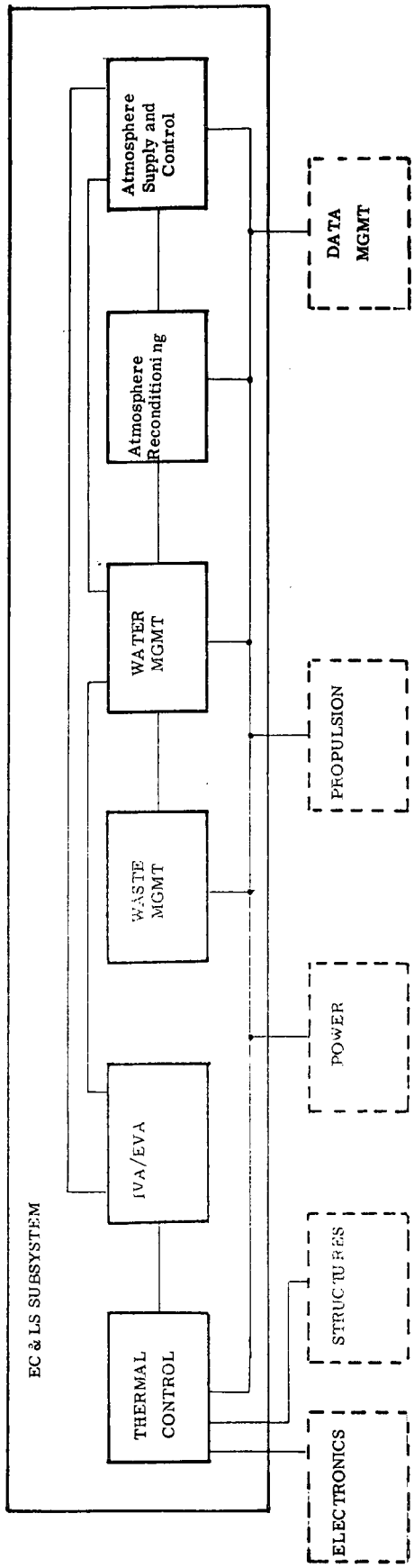

Figure 6-3. EC/LS Subsystem Interfaces

Table 6-4. EC/LS Checkout Program and Executive Program

	Task Specification	Processor Allocation	Task Termination	Memory Allocation	Peripheral Allocation	Data Base Allocation	Interrupt Monitoring	Output Processor	Input Processor	Special Processor	Data Retention	GO-NOGO Processor				
Thermal Control							x		x		x					
Atmosphere Supply							x		x		x					
Atmosphere Recond.							x				x					
Water Management							x				x					
Waste Management							x		x		x					
IVA/EVA							x	x	x		x					

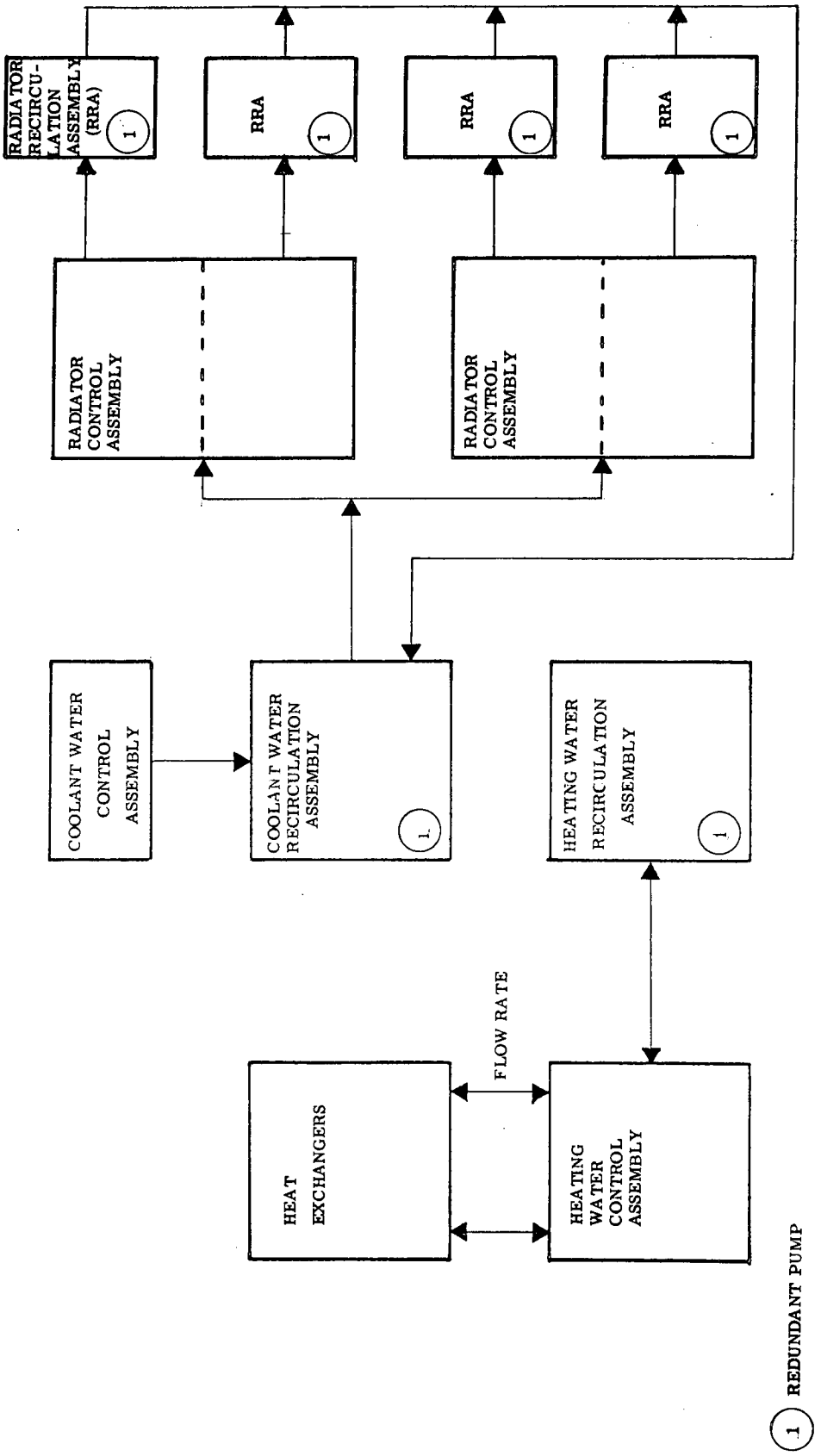

Figure 6-4. Thermal Control Assembly Group Interface

Data Management Subsystem - The data management and on-board checkout subsystems provide displays of the operational status of the EC/LS subsystem, provide spares and expendable inventory control for the EC/LS subsystem, and provide displays for fault isolation and repair.

6.2.3.2.2 Executive Program Interfaces

6.2.3.2.2.1 Input Processor

Keyboard Inputs - This program requires the capability to access parameter information input by the operator from the keyboard to specify the selection of programmed options.

6.2.3.2.2.2 Output Processor

Measure Test Points - This program requires the capability to address specific test points through the Remote Data Acquisition Units (RDAUs).

Issue Stimulus - This program requires the capability to issue stimuli to specified test points.

Display Control - This program requires the capability to present data at a display console to notify the operator of available options, or to present error messages.

6.2.3.2.2.3 Special Processor

Mode Control - This program requires the capability to have exclusive control over particular hardware components to accomplish required testing. This requires the capability to allocate a component to the program, and to permit the program to indicate a failure status on the device when an error is detected.

6.2.3.2.2.4 Miscellaneous

The IVA/EVA Assembly Group requires that the executive automatically detect when a pressure suit is attached to the system.

The Atmospheric Supply and Control Assembly Group requires access to the operational program which contains the algorithm used to determine the command issued to the cabin pressure control mechanism.

The EC/LS Subsystem requires the capability to address test points which are in a redundant capacity.

This subsystem requires direct interface (as opposed to data base interfaces) with the operational program modules.

Section 7

MAINTENANCE

There are two aspects of maintenance which entered into the basic study. Basic maintenance concepts were provided as part of the baseline resulting from the Phase B Space Station study; they are discussed in subsection 7.1 below. Additionally, one of the study tasks was aimed at implementation of an onboard electronics maintenance capability. The results of that task are summarized in subsection 7.2.

7.1 BASELINE MAINTENANCE CONCEPTS

Maintenance concepts defined for Space Station subsystems are intended to facilitate their preservation or restoration to an operational state with a minimum of time, skill, and resources within the planned environment.

7.1.1 GENERAL SPACE STATION MAINTENANCE POLICY

It is a Space Station objective that all elements be designed for a complete replacement maintenance capability unless maintainability design significantly decreases program or system reliability. This objective applies to all subsystems wherever it is reasonable to anticipate that an accident, wearout, or other failure phenomenon will significantly degrade a required function. Estimates of mean-time-between-failure, or accident/failure probability, are not accepted as prima facie evidence to eliminate a particular requirement for maintenance. Should the accident/failure probability be finite, the hardware is to be designed for replacement if it is reasonable and practical to do so.

As a design objective, no routine or planned maintenance shall require use of a pressure suit [either EVA or internal vehicular activity (IVA)] . Where manual operations in a shirtsleeve environment are impractical, remote control means of affecting such maintenance or repairs should be examined. However, EVA (or pressure suit IVA) is allowable where no other solution is reasonable, such as maintenance of external equipment.

Time dependency shall be eliminated as a factor of emergency action insofar as it is reasonable and practical to do so. This includes all program aspects of equipment, operations, and procedures which influence crew actions. When time cannot be eliminated as a factor of emergency action, a crew convenience period of 5 minutes is established as the minimum objective. The purpose of the convenience period is to provide sufficient time for deliberate, prudent, and unhurried action.

7.1.2 ONBOARD MAINTENANCE FACILITY CONCEPTS

In addition to OCS/DMS capabilities, other onboard maintenance support facilities provided on the Space Station include:

- Special tools for mission-survival contingency repairs such as soldering, metal cutting, and drilling, as determined from contingency maintenance analyses, although repairs of this type are not considered routine maintenance methods.

- Protective clothing or protective work areas for planned hazardous maintenance tasks (such as those involving fuels, etc.).

- Automated maintenance procedures and stock location data for both scheduled and unscheduled maintenance and repair activities.

- Real-time ground communication of the detailed procedures, update data, and procedures not carried onboard.

- Onboard cleanroom-type conditions by "glove box" facilities compatible with the level at which this capability is found to be required.

- Maintenance support stockrooms or stowage facilities for spares located in an area that provides for ease of inventory control and ready accessibility to docking locations or transfer passages.

7.1.3 SUBSYSTEM MAINTENANCE CONCEPTS

Space Station subsystems utilize modular concepts in design and emplacement of subsystem elements. Subsystem modularity enhances man's ability to maintain, repair, and replace elements of subsystems in orbit. Providing an effective onboard repair capability is essential in supporting the Space Station's ten-year life span since complete reliance on redundancy to achieve the long life is not feasible. The need for a repair capability, in turn, requires that a malfunction be isolated to at least its in-place remove-and-replace level. The level of fault isolation is keyed to the LRU, which is the smallest modular unit suitable for replacement. The identification of subsystem LRUs is addressed as a separate, but interdependent, part of the Onboard Checkout Study.

Specific subsystem maintenance concepts, of course, depend upon examination of the subsystems. These concepts are discussed in subsequent subparagraphs. General subsystem-related maintenance guidelines that have been established for the Space Station are:

- It is an objective to design so that EVA is not required. However, EVA may be used to accomplish maintenance/repair when no other solution is reasonable.

- Subsystems will be repaired in an in-place configuration at a level that is acceptable for safety and handling, and that can be fault-isolated and reverified by the integrated OCS/DMS. This level of maintenance is referred to as line maintenance and the module replaced to effect the repair is the LRU.

- A limited bench-level fault isolation capability will be provided on the Space Station, but is only intended for contingency (recovery of lost essential functions beyond the planned spares level) or for development purposes. Limited bench-level support is also provided in the form of standard measurement capabilities which are used primarily to reduce the amount of special test equipment required.

- Subsystem elements, wherever practical, will be replaced only at failure or wearout. Limited-life items that fail with time in a manner that can be defined by analysis and test will be allowed to operate until they have reached a predetermined level of deteriorated performance prior to replacement. Where subsystem downtimes for replacement or repair exceed desirable downtimes, the subsystem will include backup (redundant) operational capability to permit maintenance. Expendable items (filters, etc.) will be replaced on a preplanned, scheduled basis.

7.2 ONBOARD ELECTRONIC MAINTENANCE (STUDY TASK 3)

The objective of this task was to generate recommendations of supporting research and technology activities leading to implementation of a manned electronics maintenance facility for the Space Station. Early in the task it became apparent that attention could not be confined to a central maintenance facility; it was necessary to refocus the task to address implementation of an on-board maintenance capability encompassing in-place as well as centralized maintenance activities. The critical questions are the following:

- What is the optimum allocation of onboard maintenance functions between in-place and centralized maintenance facility locations?

- What is the optimum level of onboard repair (i.e., to line-replaceable unit, subassembly or module, piece part, or circuit element)?

7.2.1 MAINTENANCE CYCLE

In order to place the task in the proper context, a generalized Space Station electronic maintenance cycle is depicted in Figure 7-1.

A convenient place to enter the cycle is with detection of a fault ("In-Place Maintenance" block). The fault is isolated to a Line Replaceable Unit (LRU). The affected subsystem is restored to full capability by replacing the failed LRU with an operable one from spares storage.

The failed LRU is taken to a maintenance facility (assumed for the moment to have a fixed location in the Space Station) where it is first classified as repairable or non-repairable. Classifications will likely be predetermined, and a listing should be retained in the Data Management Subsystem. If the LRU is non-repairable, it is placed in segregated storage. If the LRU is repairable on board, the fault is further isolated to the failed Shop Replaceable Assembly (SRA). The LRU is then repaired by replacing the failed SRA with one from spares storage. The repaired LRU is then calibrated (if necessary), and its operation verified before it is placed in spares storage.

Logistics requirements (replacement LRUs and SRAs needed) are transmitted to ground-based logistics support functions by RF communications and/or Space Shuttle. Failed units are taken away from and replacement units are delivered to the Space Station by the Space Shuttle.

7.2.2 SUMMARY OF RESULTS

The study confirmed and emphasized the necessity of onboard maintenance for any manned mission of any complexity and duration measured in months (up to 10 years for Space Station). Formulation of recommendations for implementing such a capability required consideration of other topics first, and achievement of certain interim results. The principal conclusions of this study task are summarized below. The analyses leading to them are explained in the Task 3 Final Report.

- Prior studies and developments of in-space maintenance have emphasized justification of first-level (in-place) maintenance, fasteners, and tools for space application and human factors criteria. Much less attention has been devoted to test equipment, maintenance training, or definition of shop level maintenance requirements.

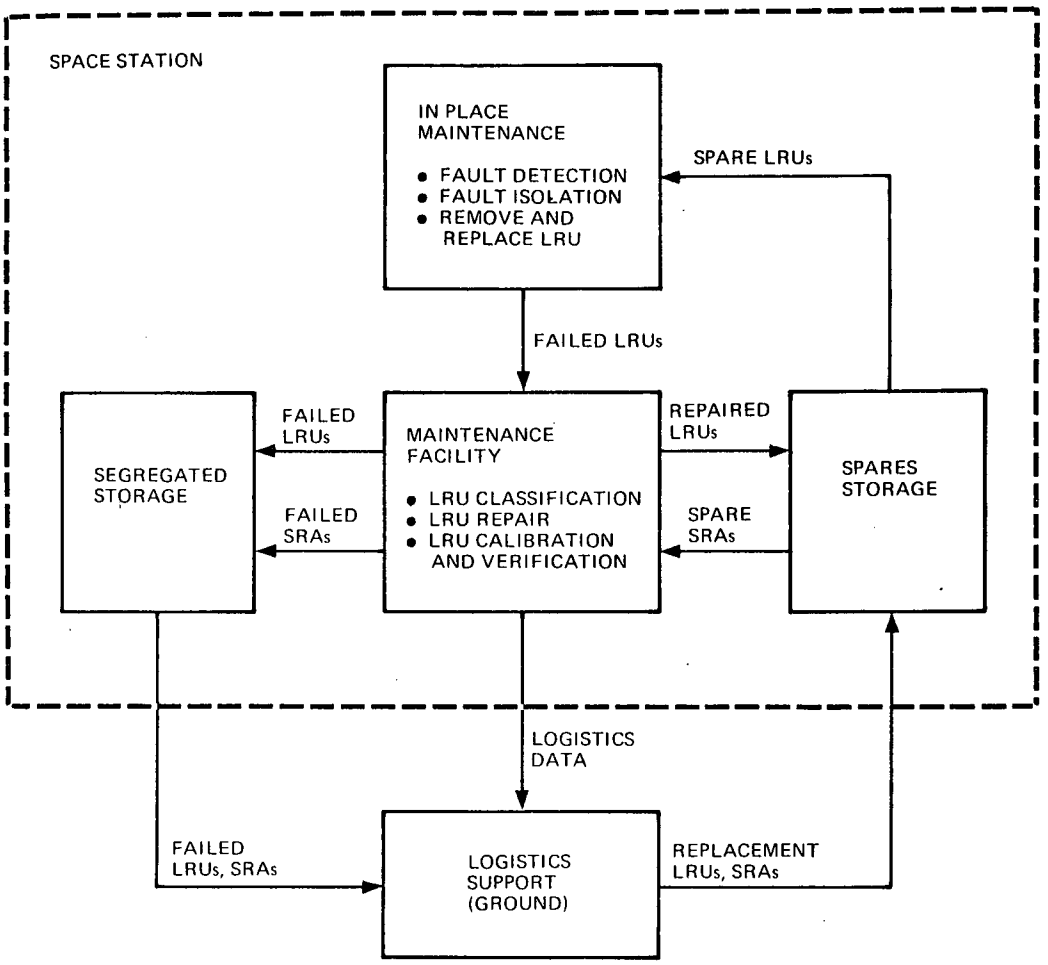

Figure 7-1. Space Station Maintenance Cycle

- The baseline subsystem descriptions, checkout requirements analysis, and software requirements analysis indicate that approximately 60 percent of all faults (over a long period) can be isolated to the failed LRU automatically under software control, without crew intervention. In an additional 27 percent of failure cases, fault isolation to one LRU can be achieved by the crew using the onboard Data Management System as a tool. In the remaining failure cases, additional fault isolation capabilities are needed. This is a good result for a "first iteration" and can probably be improved considerably with a modest effort to modify stimulus and measurement provisions.

- Crew involvement in scheduled and unscheduled maintenance (including participation in fault isolation) is estimated to average 7.2 manhours per week over the total mission time. This estimate is most sensitive to equipment reliability and levels at which onboard repair is performed. It is affected little by the efficiency of automated fault isolation under control of the Data Management Subsystem (DMS).

- The recommended approach to maintenance in the baseline Space Station is in-place removal and replacement of LRUs, without attempts to repair LRUs onboard, if the resupply interval is less than nine months. Onboard spares should be LRUs.

- For long resupply intervals or non-resupplied missions (as in a manned interplanetary mission), in-place maintenance should be by removal and replacement of LRUs. Repair of LRUs should be by removal and replacement of Shop Replaceable Assemblies (SRAs). Onboard spares should be SRAs.

- The Earth-orbital Space Station should include provision for development of onboard maintenance capability and techniques applicable to long duration non-resupplied missions and/or the larger, more complex Space Base.

- The baseline subsystem descriptions are at such a level of detail that precise specification of onboard tools and test equipment is neither feasible nor desirable. Anticipated needs identified qualitatively in the study are: (1) a portable test module to supplement software fault isolation as well as to assist mechanical adjustments and calibrator, (2) hand tools for removal and replacement of electronic assemblies, (3) devices for transporting and positioning spare assemblies, and (4) a central maintenance/repair bench.

- Several tasks have been identified and recommended for future performance, as part of a system study/design program or as separate supporting research and technology tasks. The principal ones deal with (1) development of a portable test assembly, (2) development of a repair/test bench with special provisions for small parts retention and for debris collection, (3) design for accessibility of test points and subassemblies, and (4) devices for transporting equipment within the Space Station.

The foregoing conclusions apply to the Modular Space Station as well as the 33-foot diameter, four-deck configuration.

The results of the study rest upon several assumptions and estimates, derived wherever possible from related experience. The results are not sensitive to small variations of the assumed or estimated values, except for equipment failure rates, which are most influential. Furthermore, it has not been practicable to pursue all trade analyses to include all relevant factors. Nevertheless, the study has generated valid insights into Space Station onboard maintenance and useful visibility of the path to implementation of that capability.